U.S. Department of Energy
Office of Energy Assurance

MEETING BRIEF

DOE/DHS SCADA Meeting

July 16, 2003

Prepared by:

Jack Eisenhauer
Energetics, Inc.

Table of Contents

Introduction

Supervisory control and data acquisition (SCADA) systems and digital control systems (DCS) are electronic systems used to monitor and control equipment in industrial plants and large infrastructures. They enable the remote control of sensitive processes and physical functions in industry and infrastructures that were once controlled manually. SCADA systems are used in the energy sector to control the flow of electricity in transmission and distribution lines, oil and gas in pipelines, and other energy flows within our national infrastructure. They are vital to modern energy systems because they enable efficient operation and management of large energy systems through the use of computer control. However, this very feature – automated control of interconnected energy systems – makes SCADA systems vulnerable to malicious cyber and physical attacks.

The Department of Energy's (DOE) Office of Energy Assurance (OEA) is responsible for helping to ensure a secure and reliable flow of energy to America's homes, businesses, industries, and critical infrastructures. SCADA systems have become an important feature of modern energy systems; protecting these systems from physical and cyber attack has become an important priority. Accordingly, DOE/OEA convened a meeting on July 16, 2003 with the Department of Homeland Security (DHS) and other government agencies to explore approaches for coordinating federal activities related to securing SCADA systems. This document summarizes the results of that meeting.

The Problem with SCADA Systems

Throughout the world, the U.S. energy infrastructure is envied for its reliability and robustness. However, our energy systems have become more complex in the past decade as market restructuring and technology advances have redefined how we use energy, who provides it, and where it flows. Energy companies have become quite sophisticated in managing energy operations and allocating resources to optimize their system assets. Independent system operators, aided by electronic commerce tools, have facilitated efficient wholesale energy transactions to better meet customer demands. The use of SCADA systems has enabled power providers to more easily dispatch energy to meet load requirements.

SCADA systems have become commonplace in the electric power, pipeline, water supply, and transportation systems. While physical vulnerabilities are often recognized by industry, the security risks associated with cyber vulnerabilities are less understood. Some cyber security guidelines have been provided to the energy industry but there are no universally accepted standards for SCADA security and no independent evaluation of components and systems. An additional concern is that many are built by foreign companies. The National Research Council summarized key security vulnerabilities of SCADA systems in their 2002 report on the role of science and technology in countering terrorism (see box).

One of the biggest concerns is that SCADA system development is moving away from the older hierarchical SCADA systems. The current trend is the development of open standard operating systems and distributed network-based control systems. Industry is not well prepared to address the security issues associated with these new open-standards-based control systems and the new vulnerabilities they create. Another trend is the use of open, web-based architectures to monitor and control systems, thereby opening up these systems to attack.

Security Vulnerabilities and Problems of SCADA Systems

Today's supervisory control and data acquisition (SCADA) systems have been designed with little or no attention to security. For example, data in SCADA systems are often sent "in the clear." Protocols for accepting commands are open, with no authentication required. Control channels are often wireless or leased lines that pass through commercial telecommunications facilities. For example, unencrypted radio-frequency command pathways to SCADA systems are common and, for economic reasons, the Internet itself is increasingly used as a primary command pathway. Thus, there is minimal protection against the forgery of control messages or of data and status messages. Such control paths present obvious vulnerabilities.

In addition, today's SCADA systems are built from commercial off-the-shelf components and are based on operating systems that are known to be insecure. Deregulation has meant placing a premium on the efficient use of existing capacity, and hence interconnections to shift supply from one location to another have increased. Problems of such distributed dynamic control, in combination with the complex, highly interactive nature of the system being controlled, have become major issues in operating the power grid reliably.

A final problem arises because of the real-time nature of SCADA systems, in which timing may be critical to performance and optimal efficiency (timing is important because interrupts and other operations can demand millisecond accuracy): Security add-ons in such an environment can complicate timing estimates and can cause severe degradation to SCADA performance.

Compounding the difficulty of SCADA systems' tasks is the fact that information about their vulnerability is so readily available. Such information was first brought into general view in 1998-1999, when numerous details on potential Y2K problems were put up on the World Wide Web. Additional information of greater detail—dealing with potential attacks that were directly or indirectly connected to the President's Commission on Critical Infrastructure Protection—was subsequently posted on Web pages as well. Product data and educational videotapes from engineering associations can be used to familiarize potential attackers with the basics of the grid and with specific elements. Information obtained through semiautomated reconnaissance to probe and scan the networks of a variety of power suppliers could provide terrorists with detailed information about the internals of the SCADA network, down to the level of specific makes and models of equipment used and version releases of corresponding software. And more inside information could be obtained from sympathetic engineers and operators.

Making the Nation Safer
National Research Council 2002

SCADA Systems: A National Issue

The *National Strategy to Secure Cyberspace* (2003) recognizes the vulnerabilities of SCADA systems and calls for the public and private sectors to work together to foster trusted DCS and SCADA systems. Securing these systems is important because their disruption has potential consequences for public health and safety. However, private investment in security enhancements of SCADA systems is often hard to justify. Needed research will require the talents of many operators and technology experts from several industries and infrastructures. Current technology limitations could also impede security improvements. Some security features are not easily adapted to current space or power requirements. Also, security measures could reduce performance of real-time systems.

The *Strategy* notes that SCADA systems are a widespread security issue in the energy sector and recommends several actions. It calls for an increased awareness of SCADA security issues among industry vendors and users through training, voluntary security standards, and security policies. It also notes the need to develop an adequate test bed environment and to develop technology in key areas to help secure DCS and SCADA systems.

The *Strategy* directs DHS and DOE to work in partnership with other agencies and the private sector to develop best practices and new technology to increase security of DCS/SCADA systems and to determine the most critical SCADA sites. The *Strategy* encourages a public-private partnership to secure the Nation's cyber infrastructure and recommends development of a technology and R&D gap analysis to help guide the federal cyber security research agenda.

DOE/DHS SCADA Meeting

On July 16, 2003, the Department of Energy (DOE) hosted a meeting to discuss SCADA security coordination with DHS and other federal agencies. (Meeting participants are shown in Appendix A.) The meeting had two purposes:

1) Inform DHS and other federal agencies about DOE's SCADA activities and the current state of SCADA systems in the public and private sectors.
2) Outline a path forward for a national SCADA program that optimizes federal resources.

Opening remarks were delivered by Theodore Johnson of DOE Office of Energy Assurance, John Hoyt of DHS Science and Technology Directorate, and John Cummings of DHS Science and Technology Directorate. Mr. Johnson clarified key policies and agency responsibilities that are outlined in the national strategies for homeland security. In particular, the *National Strategy to Secure Cyberspace* calls upon DOE and DHS to increase DCS/SCADA security through best practices and new technology. He emphasized the need to work with DHS and other agencies to coordinate SCADA technology efforts and maximize the national benefits from available budgets. (Mr. Johnson's presentation is provided in Appendix B).

Mr. Hoyt remarked that DHS has limited R&D funding for SCADA activities and they will be looking for early impact opportunities. Having an operational testbed for SCADA equipment would help with this objective. Mr. Cummings noted that DHS is a new entity and that coordination between the science and technology function and the operations function was critical. He viewed SCADA as the nexus between physical and cyber security.

National Laboratory Presentations

Three national laboratories – Sandia National Laboratory (SNL), Idaho National Engineering and Environmental Laboratory (INEEL), and Pacific Northwest National Laboratory (PNNL) – summarized their current activities and capabilities in SCADA security. Sandia's SCADA security activities date back to 1997 when the President's Commission on Critical Infrastructure Protection issued its report. SNL's SCADA Program includes technology R&D; testbeds, labs, and training; SCADA assessments; and security standards development. Their capabilities include a SCADA Security Development

Laboratory, test facilities, Attack Resource Centers, a SCADA Scenario Demonstration System, and related analysis and training.

INEEL has a SCADA testbed that is currently installed and being tested on its 890 square mile site. They operate their own 138 kV commercial grade power loop on the site. A secure VPN connection exists between the Sandia and Idaho testbeds. Connectivity to other government sites is been evaluated.

SNL and INEEL have proposed a National SCADA Testbed Program to help reduce vulnerabilities of SCADA systems used in energy and related infrastructures. An important function is to provide infrastructure scale testing of SCADA security solutions and serve as a full-scale honest broker to validate systems. The Testbed is envisioned as a virtual environment that connects SNL and INEEL, as well as other potential sites.

PNNL has been involved with DOE's Infrastructure Assurance Outreach Program since 1996. In 1999, researchers at PNNL established a SCADA research laboratory using laboratory directed research and development (LDRD) funding, with protocol analyzers and other test equipment. PNNL has leveraged this effort with its work for other agencies and partners to identify specific vulnerabilities, raise awareness, and to demonstrate countermeasures to improve SCADA security. PNNL has been active in industry forums and work groups that address SCADA security, including those led by the North American Electric Reliability Council (NERC), the National Institute of Standards and Technology (NIST), the Instrumentation Society of America (ISA), and the Electric Power Research Institute (EPRI).

The SNL and INEEL presentations are provided in Appendix B.

Discussion

The meeting participants were asked three fundamental questions following the laboratory presentations:

- Does a National SCADA Test Bed Make Sense?
- How Do We Get the Most Out of a National SCADA Program?
- How Do We Proceed?

A key issue concerned the scope of a national SCADA program. Should it encompass all infrastructures? Should it focus initially on energy SCADA systems? Should it cover testing, validation, certification, technology adoption, research, and/or development? Should it include international partners? Does it duplicate efforts in the private sector?

A range of opinions were voiced regarding these questions with no clear consensus. However, most people felt that a more focused effort was needed in the near-term to achieve tangible results. For example, the effort might focus initially on testing and validating energy SCADA systems without international partners. Many supported the idea of a more comprehensive national SCADA effort in the longer term.

To get the most out of a national SCADA program, good coordination will be needed between DHS and DOE, and with other federal agencies and industrial partners. One issue is how to bring other industries into this activity. Another question is how best to organize and manage a national SCADA effort. Should it include an advisory group? Should a joint program office be established? How will it coordinate with other test beds?

Next Steps

Although the discussion raised many issues that could not be addressed in the allotted time, the principals agreed on several next steps.

- Establish a joint DOE-DHS effort on SCADA security for the energy sector
- Examine options for program management and advisory groups
- Determine how best to engage stakeholders
- Assess the near- and long-term SCADA requirements within DOE and DHS

Notes from the discussion are shown below.

Discussion Notes – DOE/DHS SCADA Meeting

<table>
<tr><th>Does A National SCADA Test Bed Make Sense?</th><th>How Do We Get the Most Out of A National SCADA Program?</th></tr>
<tr><td rowspan="3">• Emphasis on national → addresses clear needs and gaps
• How to convince industry of urgency
• Educational element is important
• Need a complement to WMD effort
• Need a team approach → converge capabilities
• Too scattered → need a “head”
• Not just testing and validating → next step is also important
• Need to show clear, tangible results and benefits
• Need to pull in the key stakeholders
• Should migrate from government funding to private funding
• Interdependency relationships need to be examined
• Broaden capability → beyond U.S., Canada, UK
• How to expand beyond energy to other areas (e.g., water)
• How to best coordinate effort
• When are we done?
• Technology transition is critical
• Industry outreach is important
• Technology adoption should be a major focus
• Raising awareness is critical at several levels
• Testing is not the end product → how to develop new technology</td><td>• Key players
– Bring in other industries → how to do it (ex: military refueling system)
– Need to establish trust with industry
• Funding
• Organization and management
– Joint program office?
– How to coordinate with other test beds?
– Advisory committee plus program office
– Executive secretariat
– Should it be confined to energy?</td></tr>
<tr><td><b>• How Do We Proceed?</b></td></tr>
<tr><td>• Establish a joint DOE-DHS effort for SCADA with energy
• Examine options for program management and advisory groups
• Determine how best to engage stakeholders
• Assess separate near-term and long-term requirements</td></tr>
</table>

APPENDICES

Appendix A

DOE/DHS SCADA Meeting

July 16, 2003

Energetics
901 D Street SW, Suite 100
Washington, DC

Participants

Dale Barr, DHS National Communications System, Barrd@ncs.gov, 703.607.6157

Tommy Cabe, Sandia National Laboratories/DOE Office of Energy Assurance, Tommy.Cabe@hq.doe.gov, 202.586.1273

John Cummings, DHS, john.cummings@dhs.gov, 202.772.9537

John Hoyt, DHS, john.hoyt@dhs.gov, 202.772.9959

Theodore Johnson, DOE Office of Energy Assurance, Theodore.Johnson@hq.doe.gov, 202.586.6937

D.R. Miles, Pacific Northwest National Laboratory, dr.miles@pnl.gov, 509.372.4515

John Noon, Idaho National Engineering and Environmental Laboratory, noonjj@inel.gov, 208.526.1165

Perry Pederson, Technology Support Working Group, pedersonp@tswg.gov, 703.602.6215

Frederick Proctor, National Institute of Standards and Technology, proctor@cme.nist.gov, 301.975.3425

Gary Seifert, Idaho National Engineering and Environmental Laboratory, sei@inel.gov, 208.526.9522

Jimmy Scott, Wintech, scott@tswg.gov, 703.604.1681

Michael Skroch, Sandia National Laboratories, mjskroc@sandia.gov, 505.844.0104

Michael Smith, Defense Intelligence Agency, michael.smith@dia.mil, 702.499.6708

Mike Soboroff, DOE Office of Energy Assurance, mike.soboroff@hq.doe.gov, 202.586.4936

Juan Torres, Sandia National Laboratories, jjtorre@sandia.gov, 505.844.0809

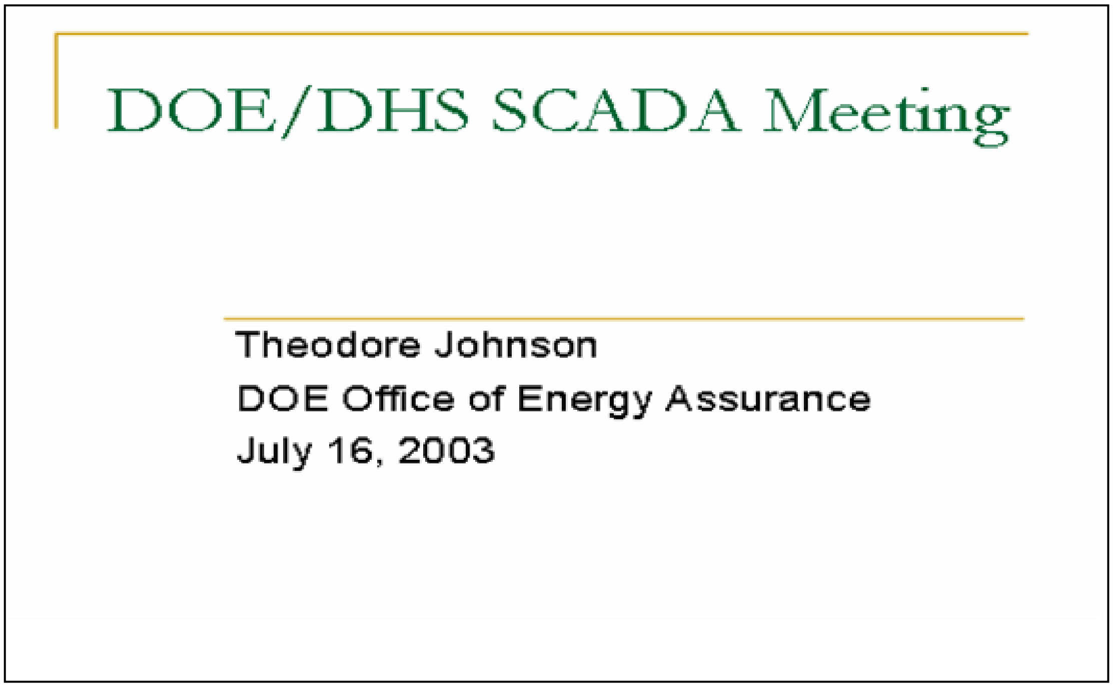
Kenneth Watts, Idaho National Engineering and Environmental Laboratory, kdw@inel.gov, 208.526.9628

Facilitators

Jack Eisenhauer, Energetics, jeisenhauer@energetics.com, 410.953.6246

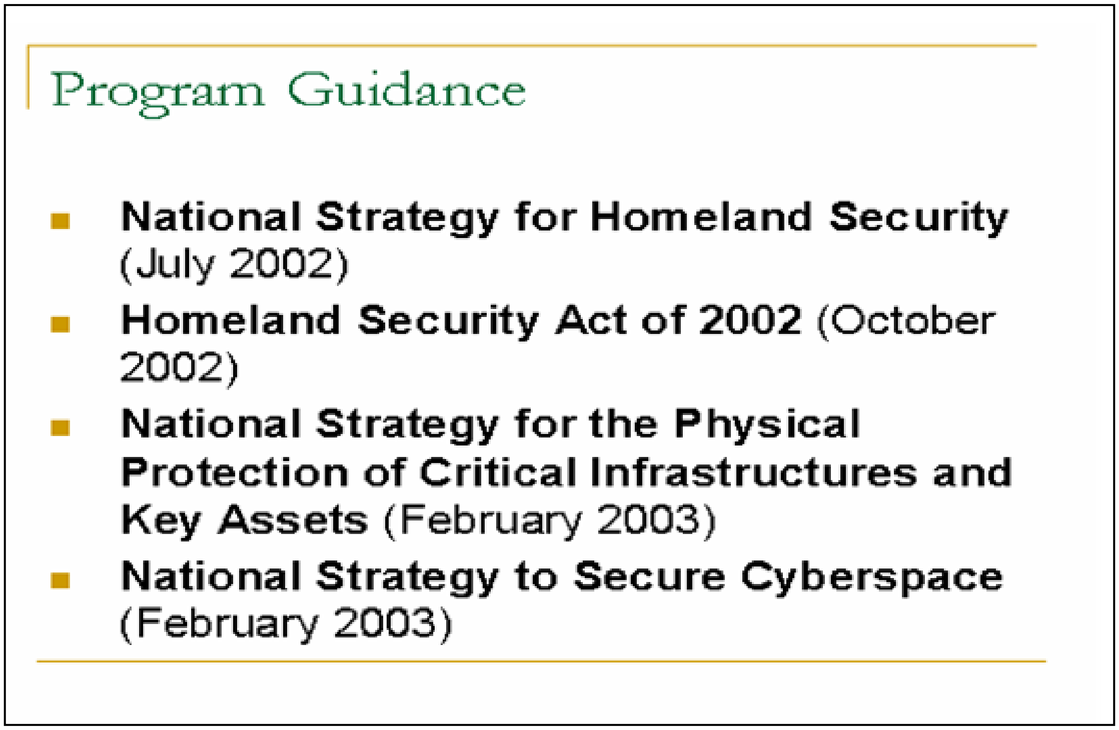
Jamie Lyons, Energetics, jlyons@energetics.com, 410.953.6281

Appendix B - Presentations



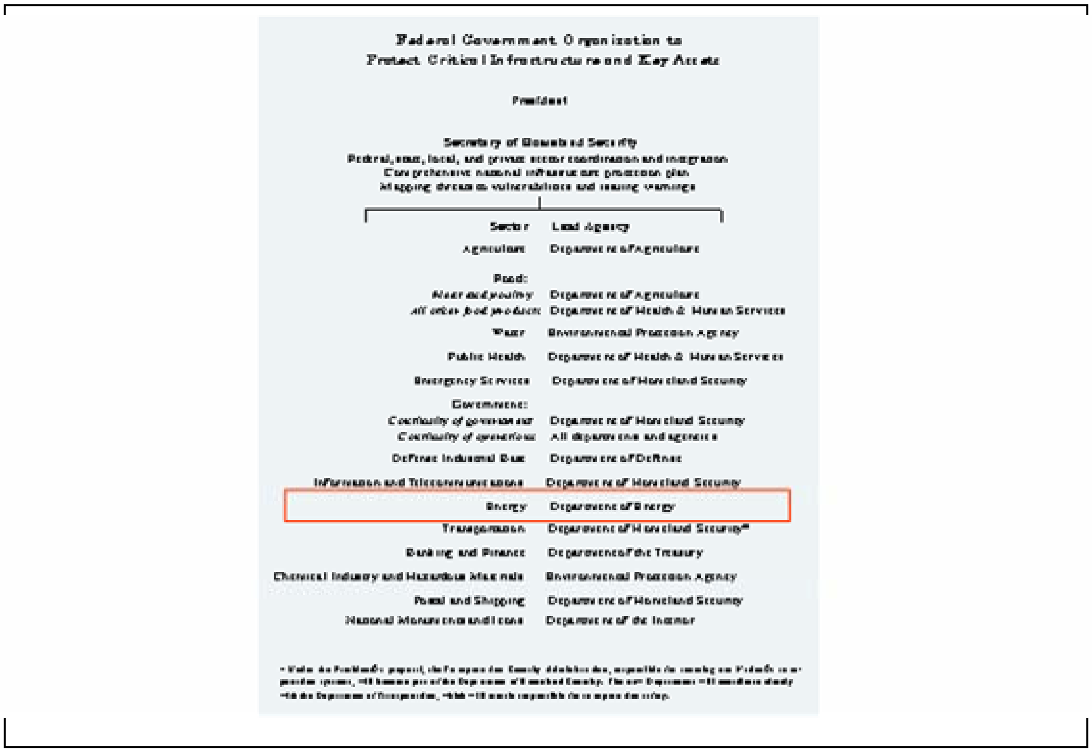
DOE/DHS SCADA Meeting

Theodore Johnson
DOE Office of Energy Assurance
July 16, 2003



Program Guidance

- **National Strategy for Homeland Security** (July 2002)
- **Homeland Security Act of 2002** (October 2002)
- **National Strategy for the Physical Protection of Critical Infrastructures and Key Assets** (February 2003)
- **National Strategy to Secure Cyberspace** (February 2003)



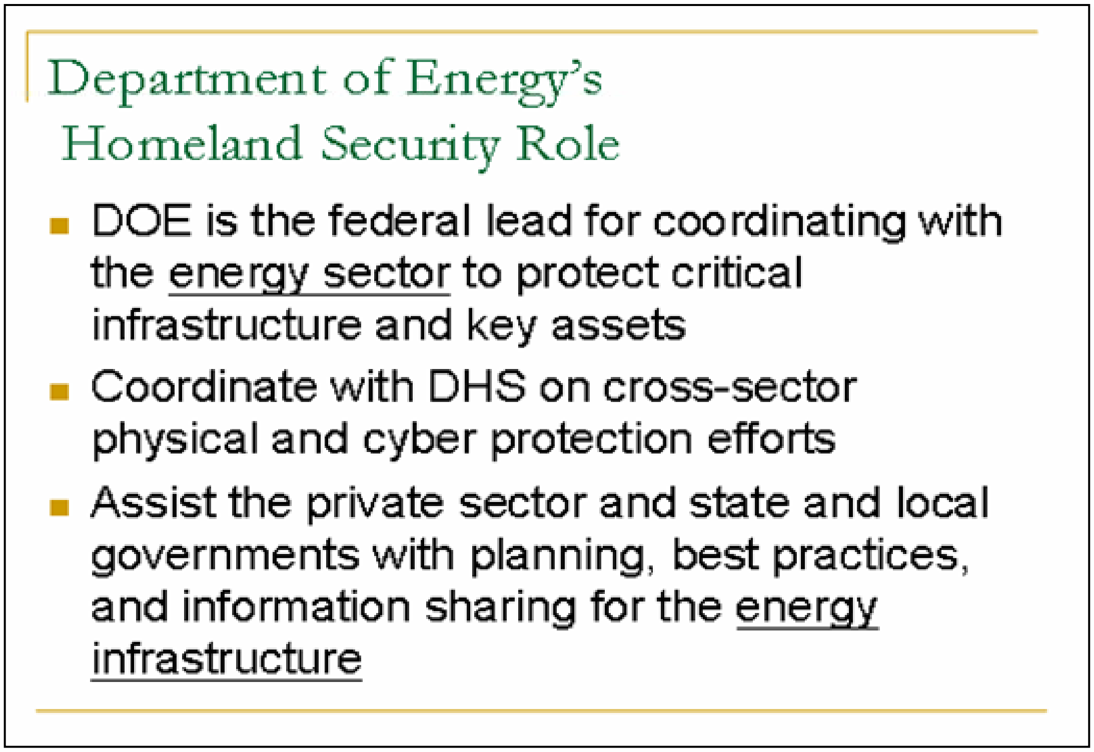
Federal Government Organization to Protect Critical Infrastructure and Key Assets

President

Secretary of Homeland Security
Federal, state, local, and private sector coordination and integration
Comprehensive national infrastructure protection plan
Mapping threats to vulnerabilities and issuing warnings

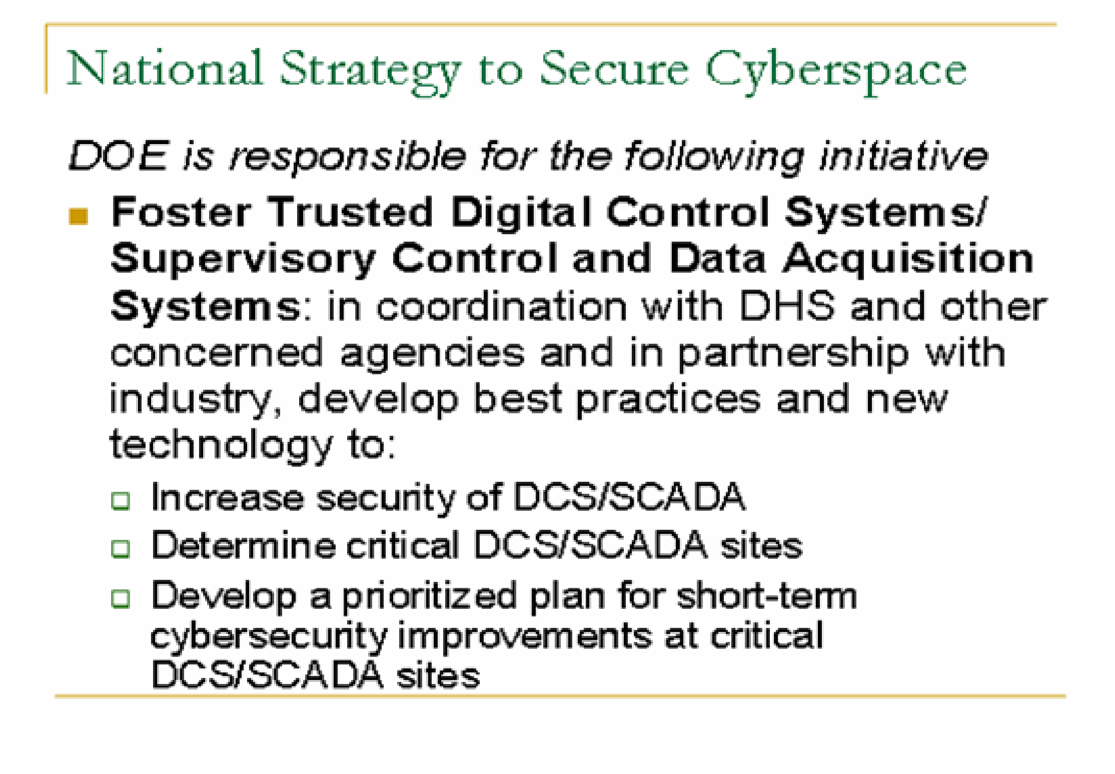
Sector	Lead Agency
Agriculture	Department of Agriculture
Food:	
Meat and poultry	Department of Agriculture
All other food products	Department of Health & Human Services
Water	Environmental Protection Agency
Public Health	Department of Health & Human Services
Emergency Services	Department of Homeland Security
Government:	
Continuity of government	Department of Homeland Security
Continuity of operations	All departments and agencies
Defense Industrial Base	Department of Defense
Information and Telecommunications	Department of Homeland Security
Energy	Department of Energy
Transportation	Department of Homeland Security*
Banking and Finance	Department of the Treasury
Chemical Industry and Hazardous Materials	Environmental Protection Agency
Postal and Shipping	Department of Homeland Security
National Monuments and Icons	Department of the Interior

* Under the President's proposal, the Transportation Security Administration, responsible for securing our Nation's transportation systems, will become part of the Department of Homeland Security. The new Department will coordinate closely with the Department of Transportation, which will remain responsible for transportation safety.



Department of Energy's Homeland Security Role

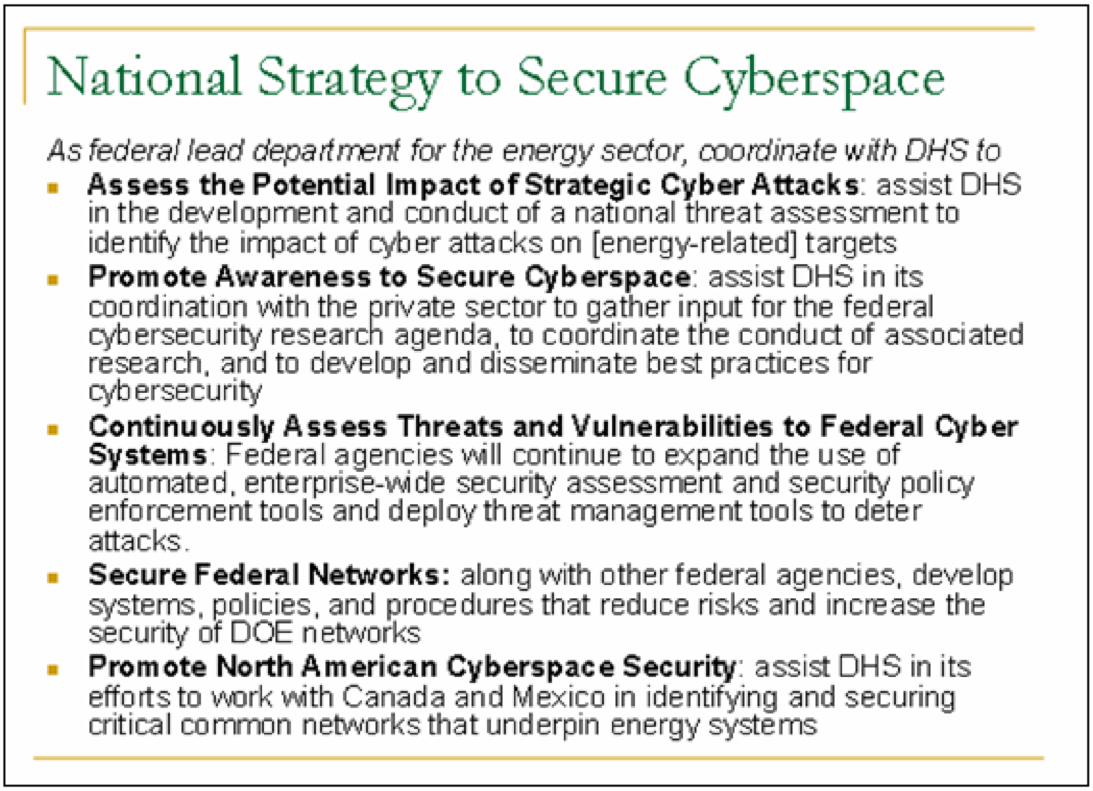
- DOE is the federal lead for coordinating with the energy sector to protect critical infrastructure and key assets
- Coordinate with DHS on cross-sector physical and cyber protection efforts
- Assist the private sector and state and local governments with planning, best practices, and information sharing for the energy infrastructure



National Strategy to Secure Cyberspace

DOE is responsible for the following initiative

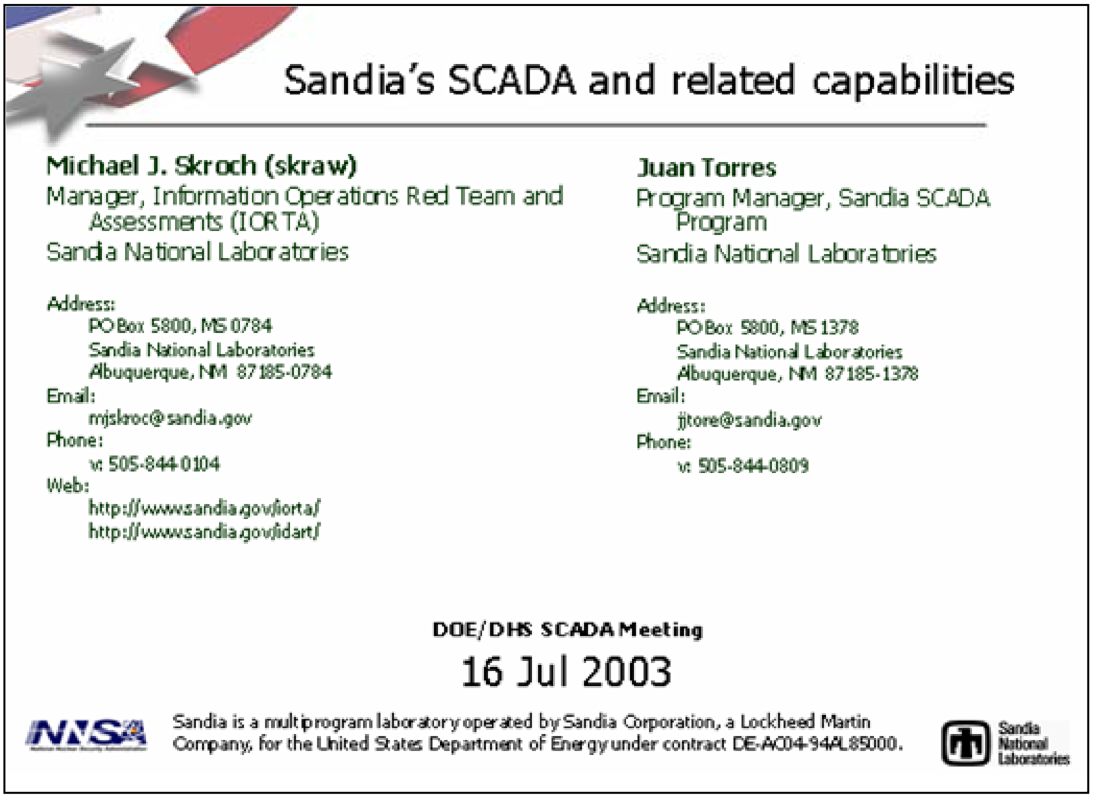
- **Foster Trusted Digital Control Systems/ Supervisory Control and Data Acquisition Systems**: in coordination with DHS and other concerned agencies and in partnership with industry, develop best practices and new technology to:
  - ☐ Increase security of DCS/SCADA
  - ☐ Determine critical DCS/SCADA sites
  - ☐ Develop a prioritized plan for short-term cybersecurity improvements at critical DCS/SCADA sites



National Strategy to Secure Cyberspace

As federal lead department for the energy sector, coordinate with DHS to

- **Assess the Potential Impact of Strategic Cyber Attacks**: assist DHS in the development and conduct of a national threat assessment to identify the impact of cyber attacks on [energy-related] targets
- **Promote Awareness to Secure Cyberspace**: assist DHS in its coordination with the private sector to gather input for the federal cybersecurity research agenda, to coordinate the conduct of associated research, and to develop and disseminate best practices for cybersecurity
- **Continuously Assess Threats and Vulnerabilities to Federal Cyber Systems**: Federal agencies will continue to expand the use of automated, enterprise-wide security assessment and security policy enforcement tools and deploy threat management tools to deter attacks.
- **Secure Federal Networks:** along with other federal agencies, develop systems, policies, and procedures that reduce risks and increase the security of DOE networks
- **Promote North American Cyberspace Security**: assist DHS in its efforts to work with Canada and Mexico in identifying and securing critical common networks that underpin energy systems



Sandia's SCADA and related capabilities

Michael J. Skroch (skraw)
Manager, Information Operations Red Team and Assessments (IORTA)
Sandia National Laboratories

Address:
PO Box 5800, MS 0784
Sandia National Laboratories
Albuquerque, NM 87185-0784
Email:
mjskroc@sandia.gov
Phone:
v: 505-844-0104
Web:
http://www.sandia.gov/iorta/
http://www.sandia.gov/idart/

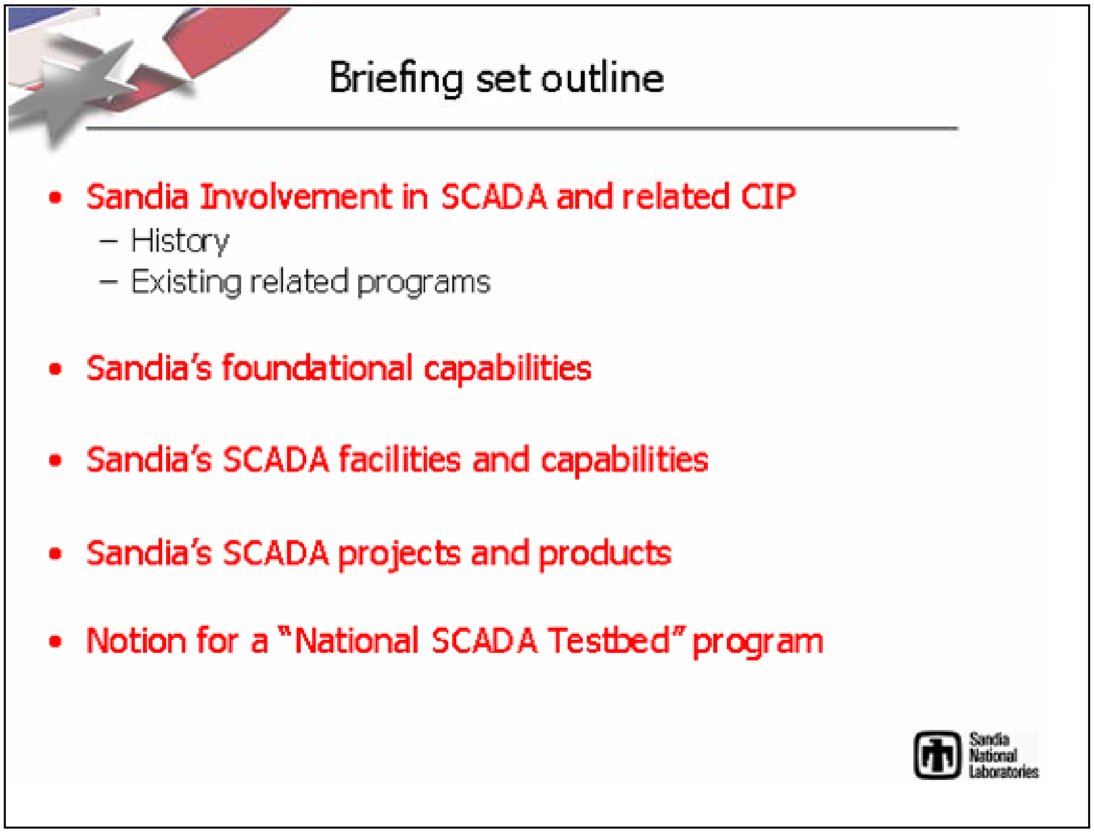
Juan Torres
Program Manager, Sandia SCADA Program
Sandia National Laboratories

Address:
PO Box 5800, MS 1378
Sandia National Laboratories
Albuquerque, NM 87185-1378
Email:
jjtore@sandia.gov
Phone:
v: 505-844-0809

DOE/DHS SCADA Meeting

16 Jul 2003

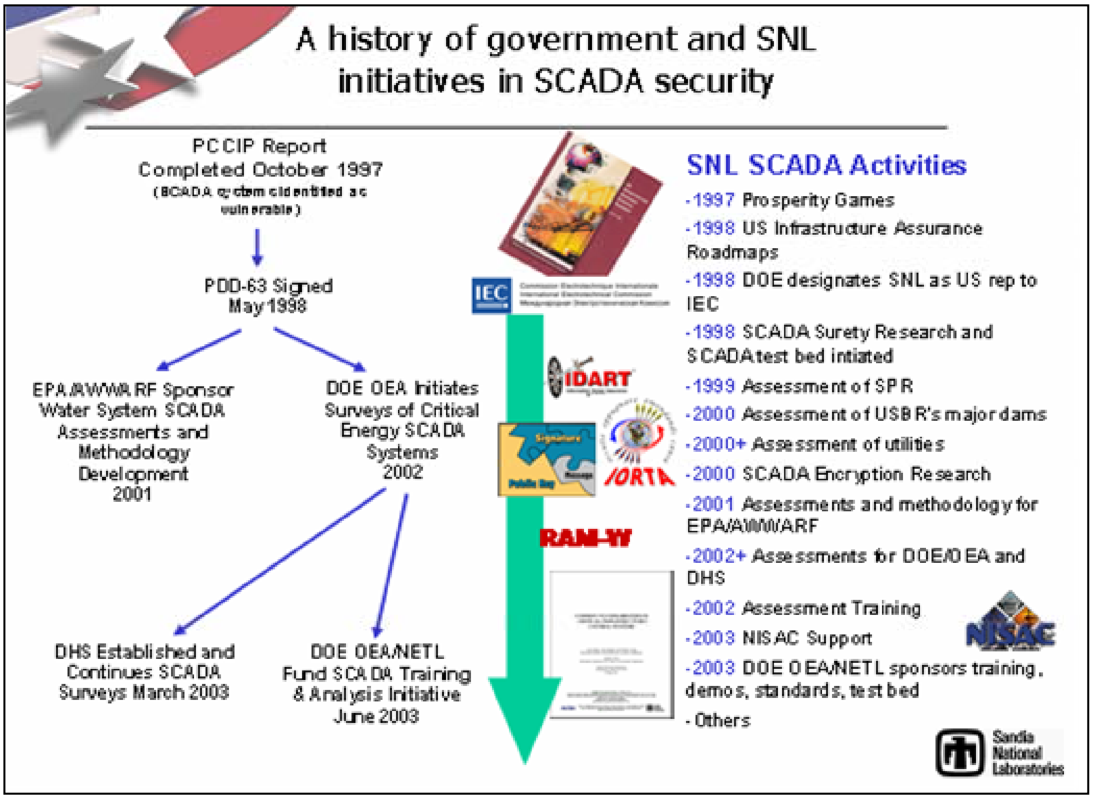
Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under contract DE-AC04-94AL85000.



Briefing set outline

- Sandia Involvement in SCADA and related CIP
  - History
  - Existing related programs
- Sandia's foundational capabilities
- Sandia's SCADA facilities and capabilities
- Sandia's SCADA projects and products
- Notion for a "National SCADA Testbed" program

Sandia has programs that address surety of critical infrastructures



A history of government and SNL initiatives in SCADA security

PCCIP Report
Completed October 1997
(SCADA system identified as vulnerable)

PDD-63 Signed
May 1998

EPA/AWWARF Sponsor Water System SCADA Assessments and Methodology Development 2001

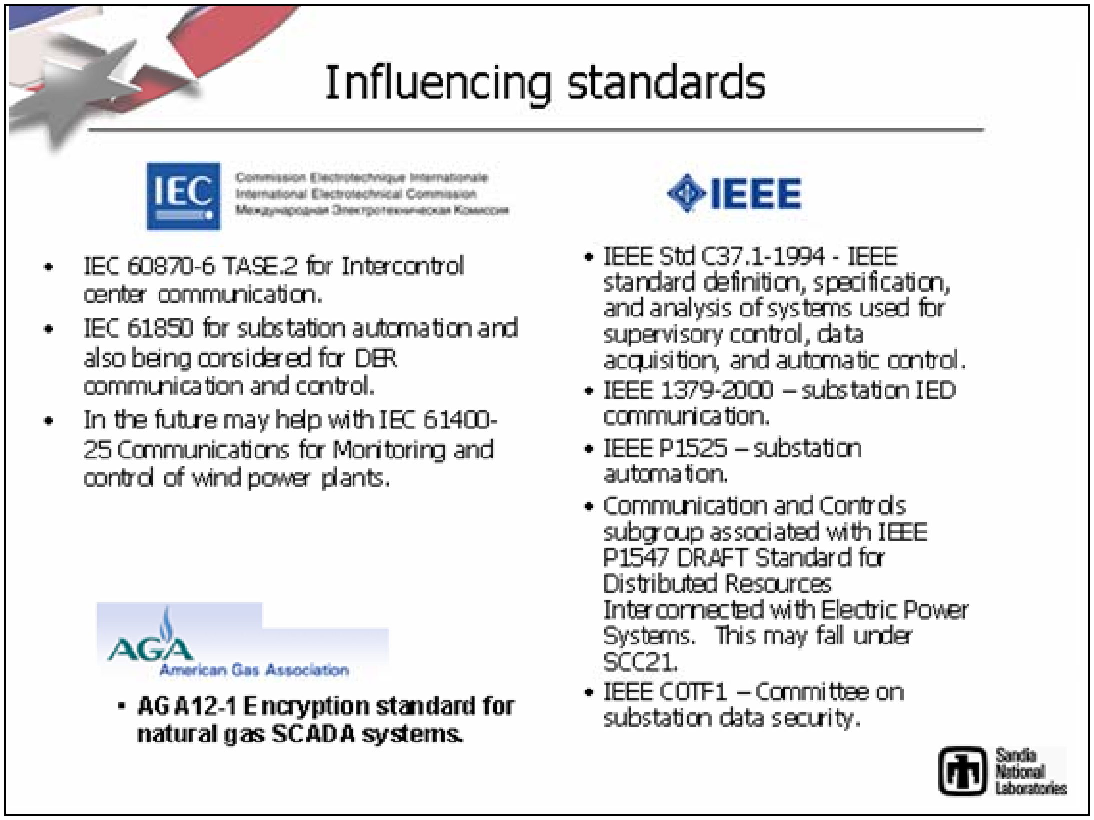
DOE OEA Initiates Surveys of Critical Energy SCADA Systems 2002

DHS Established and Continues SCADA Surveys March 2003

DOE OEA/NETL Fund SCADA Training & Analysis Initiative June 2003

SNL SCADA Activities

- 1997 Prosperity Games
- 1998 US Infrastructure Assurance Roadmaps
- 1998 DOE designates SNL as US rep to IEC
- 1998 SCADA Surety Research and SCADA test bed intiated
- 1999 Assessment of SPR
- 2000 Assessment of USBR's major dams
- 2000+ Assessment of utilities
- 2000 SCADA Encryption Research
- 2001 Assessments and methodology for EPA/AWWARF
- 2002+ Assessments for DOE/OEA and DHS
- 2002 Assessment Training
- 2003 NISAC Support
- 2003 DOE OEA/NETL sponsors training, demos, standards, test bed
- Others



Influencing standards

IEC
Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

- IEC 60870-6 TASE.2 for Intercontrol center communication.
- IEC 61850 for substation automation and also being considered for DER communication and control.
- In the future may help with IEC 61400-25 Communications for Monitoring and control of wind power plants.

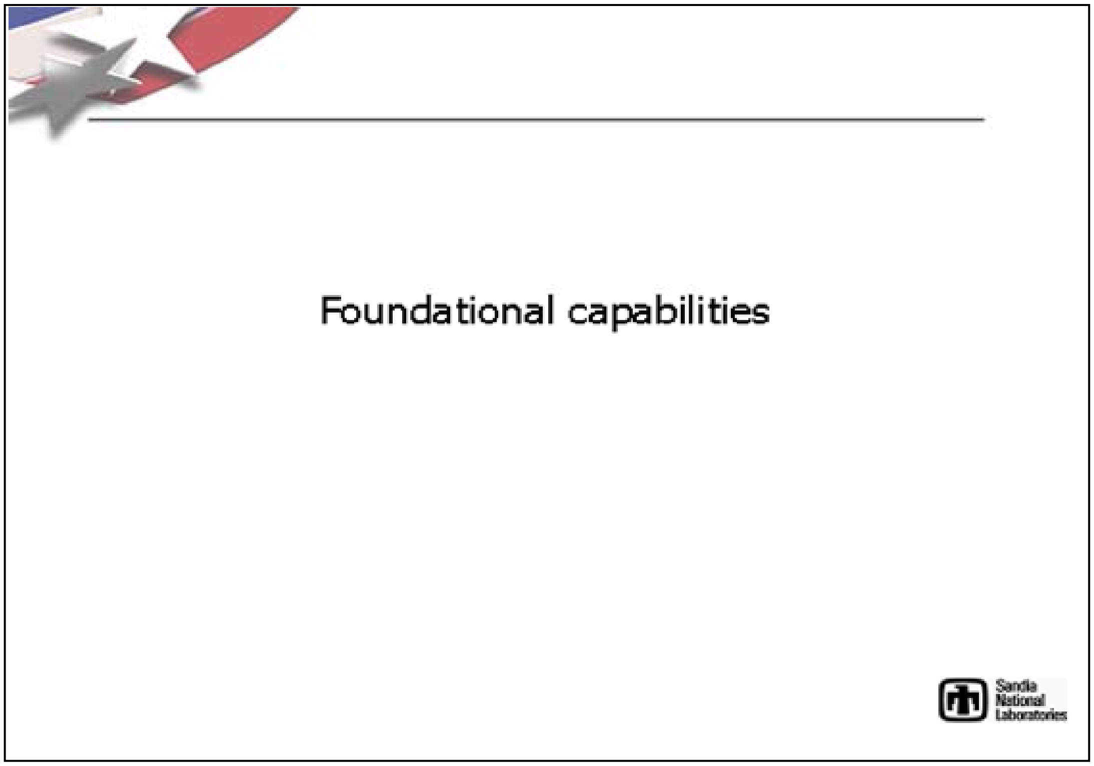
AGA
American Gas Association

- **AGA12-1 Encryption standard for natural gas SCADA systems.**

IEEE

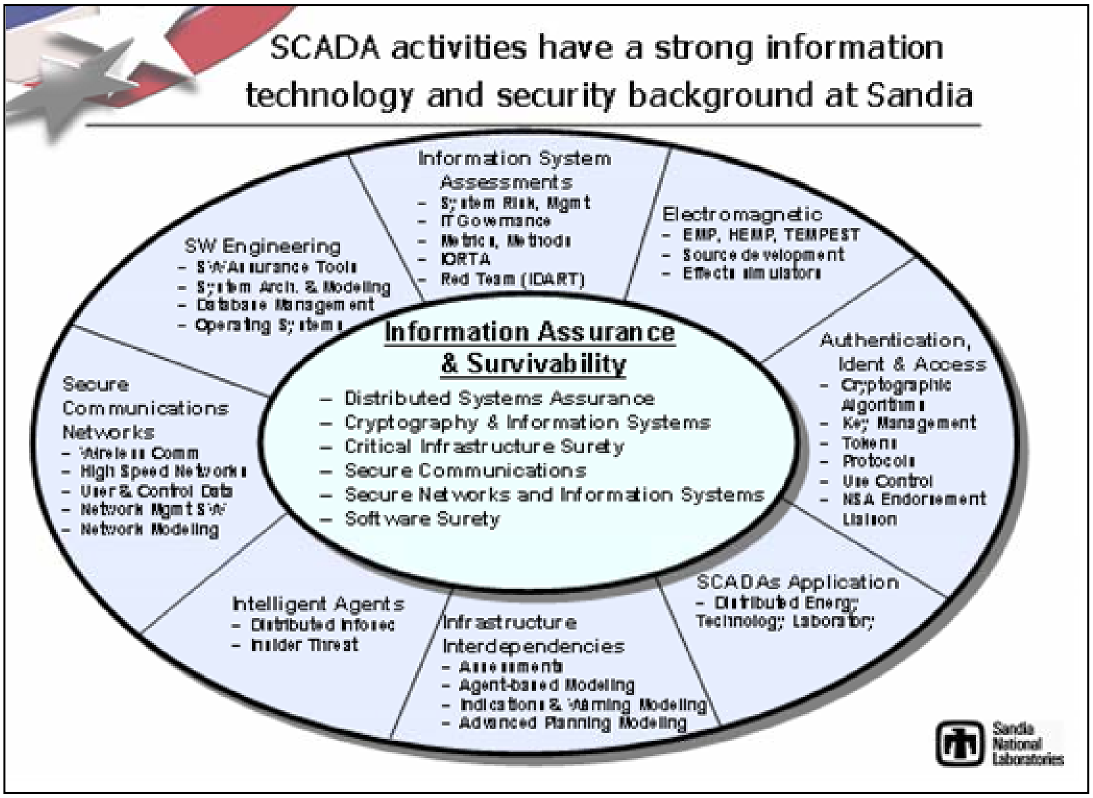
- IEEE Std C37.1-1994 - IEEE standard definition, specification, and analysis of systems used for supervisory control, data acquisition, and automatic control.
- IEEE 1379-2000 – substation IED communication.
- IEEE P1525 – substation automation.
- Communication and Controls subgroup associated with IEEE P1547 DRAFT Standard for Distributed Resources Interconnected with Electric Power Systems. This may fall under SCC21.
- IEEE COTF1 – Committee on substation data security.

Sandia National Laboratories



Foundational capabilities

Sandia National Laboratories



SCADA activities have a strong information technology and security background at Sandia

Information Assurance & Survivability

- Distributed Systems Assurance
- Cryptography & Information Systems
- Critical Infrastructure Surety
- Secure Communications
- Secure Networks and Information Systems
- Software Surety

Information System Assessments
- System Risk, Mgmt
- IT Governance
- Metrics, Methods
- IORTA
- Red Team (IDART)

Electromagnetic
- EMP, HEMP, TEMPEST
- Source development
- Effects simulators

Authentication, Ident & Access
- Cryptographic Algorithms
- Key Management
- Tokens
- Protocols
- Use Control
- NSA Endorsement Liaison

SCADAs Application
- Distributed Energy Technology Laboratory

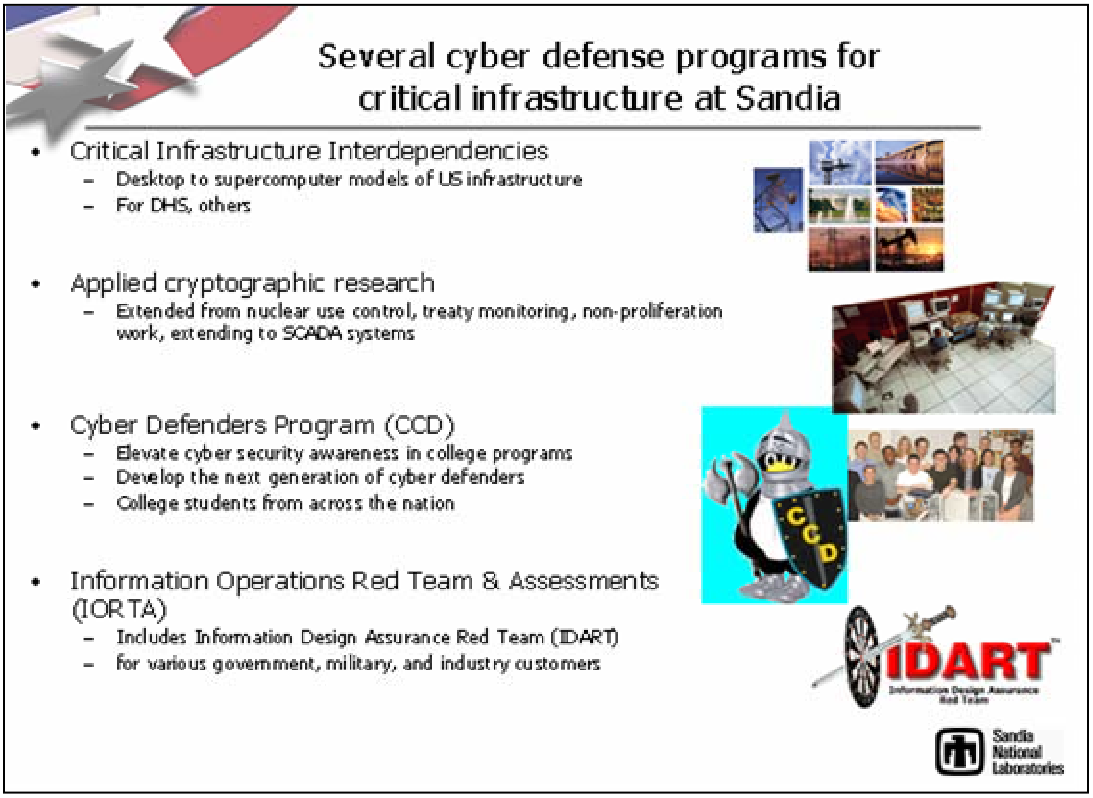
Infrastructure Interdependencies
- Assessments
- Agent-based Modeling
- Indications & Warning Modeling
- Advanced Planning Modeling

Intelligent Agents
- Distributed Infosec
- Insider Threat

Secure Communications Networks
- Wireless Comm
- High Speed Networks
- User & Control Data
- Network Mgmt SW
- Network Modeling

SW Engineering
- SW Assurance Tools
- System Arch. & Modeling
- Database Management
- Operating Systems

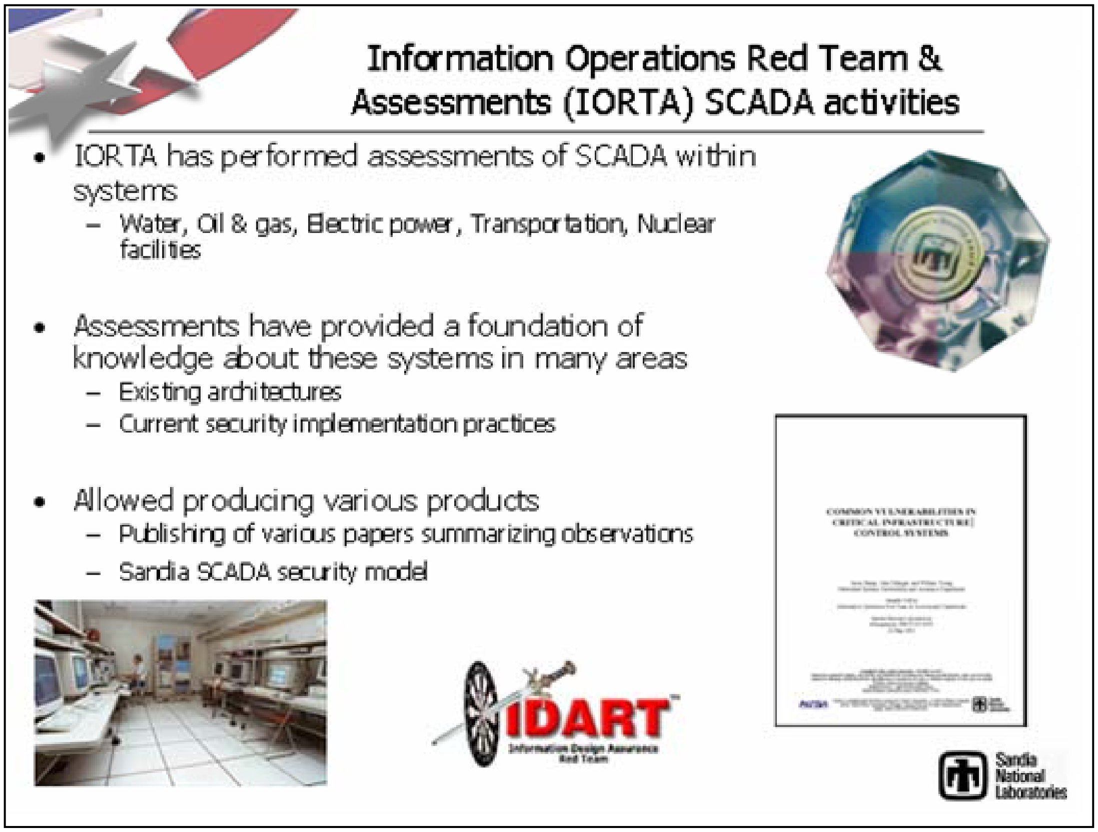
Sandia National Laboratories



Several cyber defense programs for critical infrastructure at Sandia

- Critical Infrastructure Interdependencies
  - Desktop to supercomputer models of US infrastructure
  - For DHS, others
- Applied cryptographic research
  - Extended from nuclear use control, treaty monitoring, non-proliferation work, extending to SCADA systems
- Cyber Defenders Program (CCD)
  - Elevate cyber security awareness in college programs
  - Develop the next generation of cyber defenders
  - College students from across the nation
- Information Operations Red Team & Assessments (IORTA)
  - Includes Information Design Assurance Red Team (IDART)
  - for various government, military, and industry customers

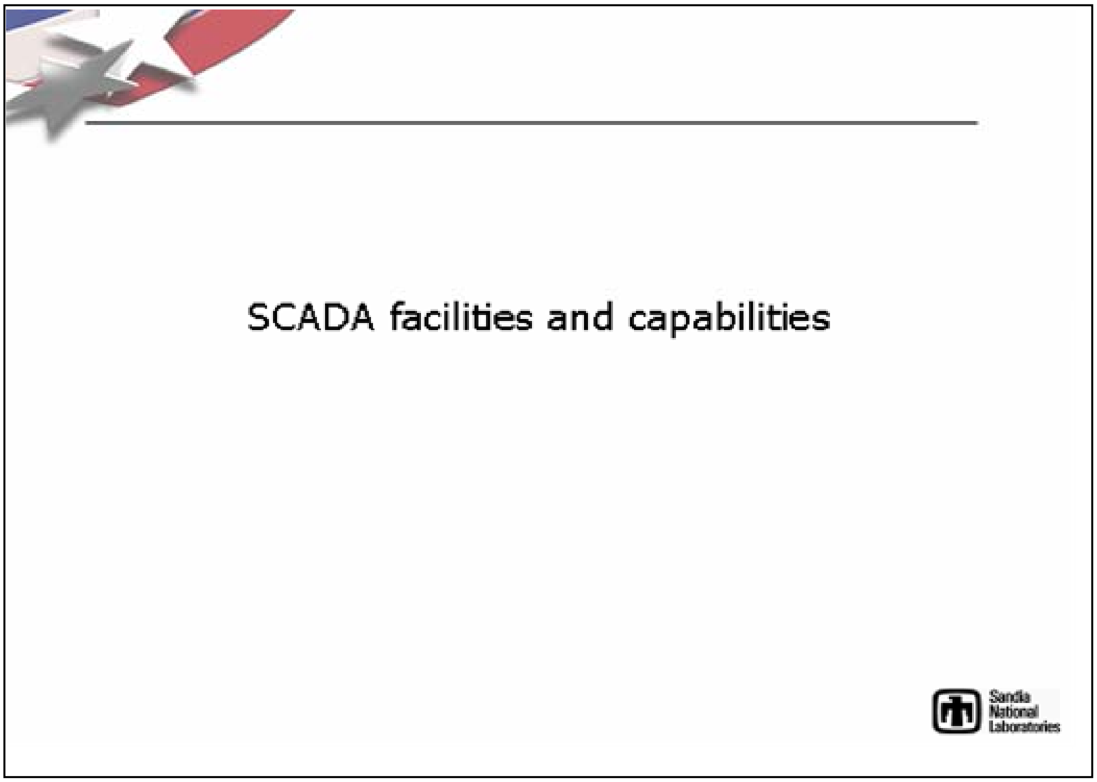
CCD
IDART™
Information Design Assurance Red Team
Sandia National Laboratories



Information Operations Red Team & Assessments (IORTA) SCADA activities

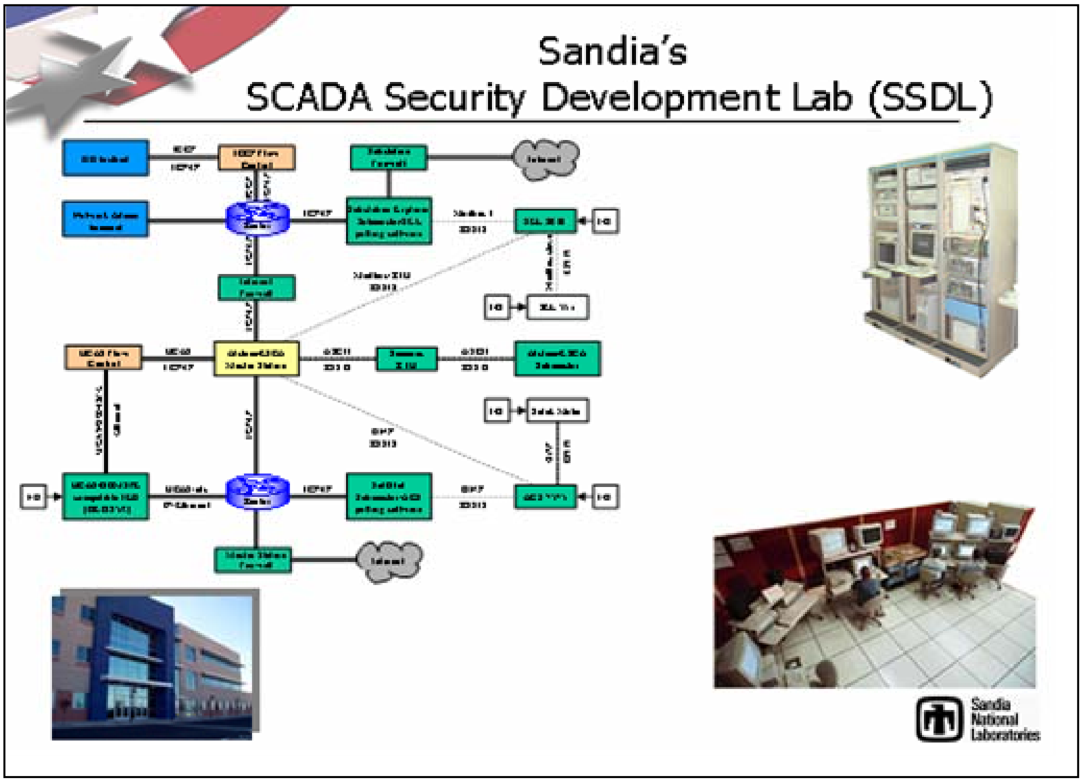
- IORTA has performed assessments of SCADA within systems
  - Water, Oil & gas, Electric power, Transportation, Nuclear facilities
- Assessments have provided a foundation of knowledge about these systems in many areas
  - Existing architectures
  - Current security implementation practices
- Allowed producing various products
  - Publishing of various papers summarizing observations
  - Sandia SCADA security model

COMMON VULNERABILITIES IN CRITICAL INFRASTRUCTURE CONTROL SYSTEMS
IDART™
Information Design Assurance Red Team
Sandia National Laboratories



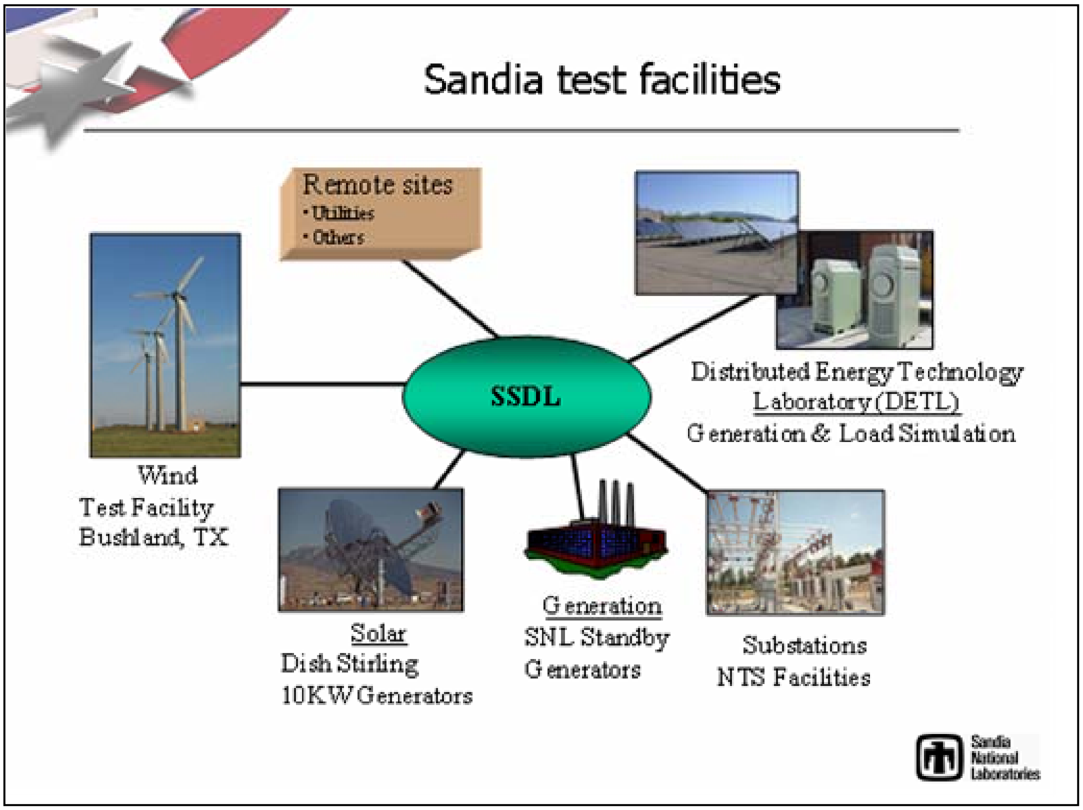
SCADA facilities and capabilities

Sandia National Laboratories



Sandia's SCADA Security Development Lab (SSDL)

Sandia National Laboratories



Sandia test facilities

Remote sites
- Utilities
- Others

SSDL

Wind Test Facility Bushland, TX

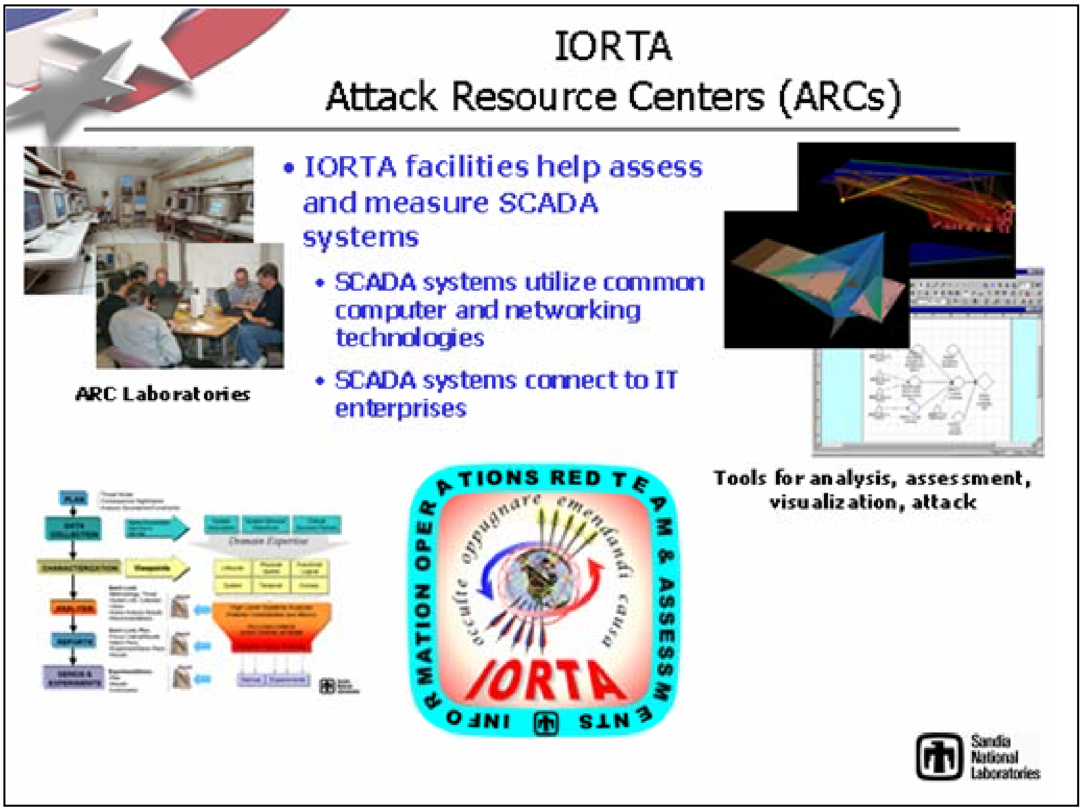
Solar Dish Stirling 10KW Generators

Generation SNL Standby Generators

Distributed Energy Technology Laboratory (DETL) Generation & Load Simulation

Substations NTS Facilities

Sandia National Laboratories



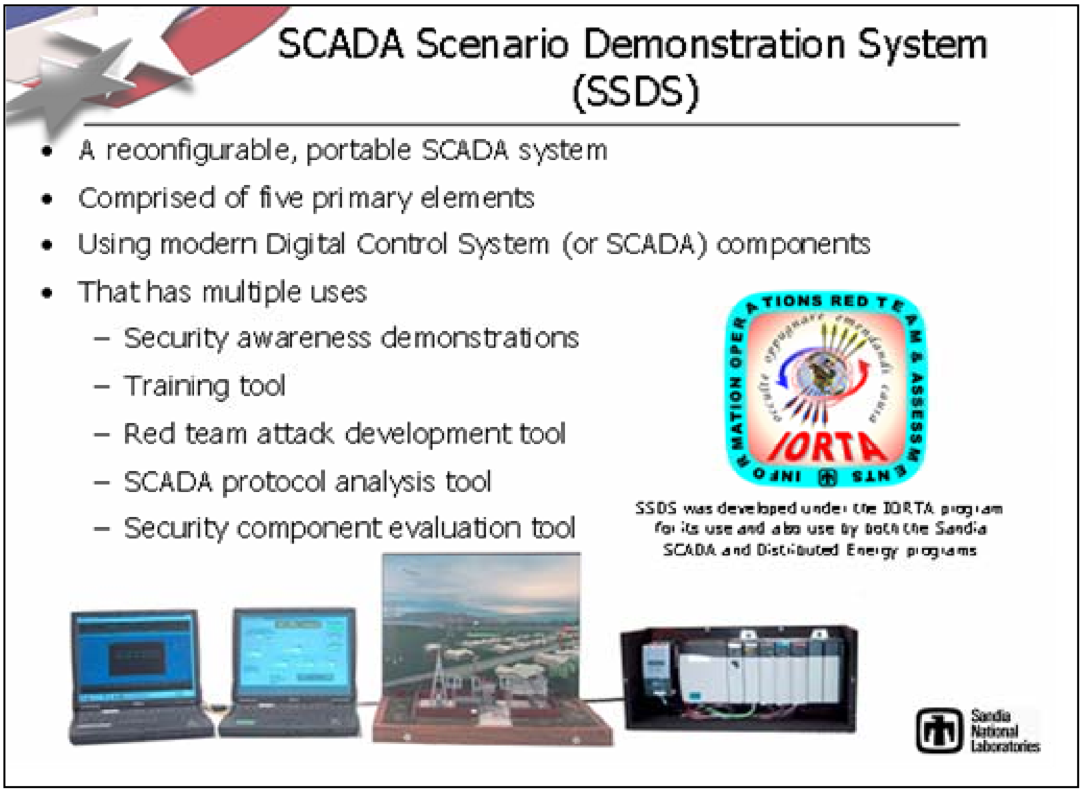
IORTA Attack Resource Centers (ARCs)

- IORTA facilities help assess and measure SCADA systems
  - SCADA systems utilize common computer and networking technologies
  - SCADA systems connect to IT enterprises

ARC Laboratories

Tools for analysis, assessment, visualization, attack

INFORMATION OPERATIONS RED TEAM & ASSESSMENTS
occulte oppugnare emendandi causa
IORTA
Domain Expertise
Sandia National Laboratories

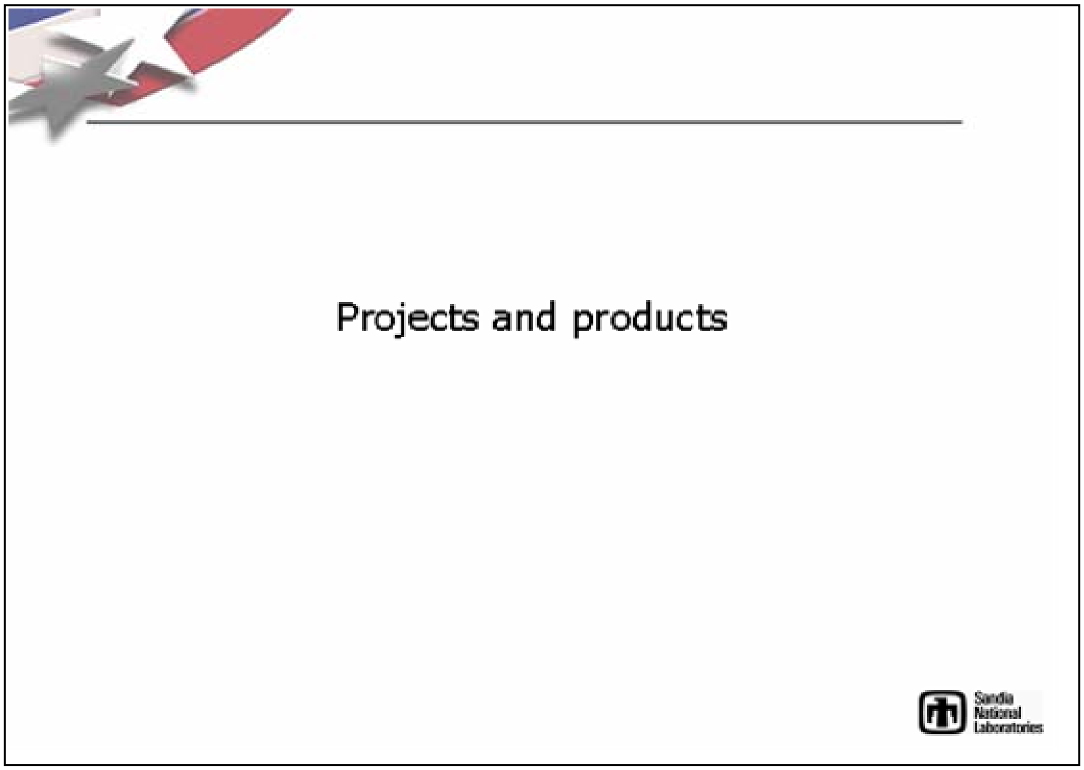


SCADA Scenario Demonstration System (SSDS)

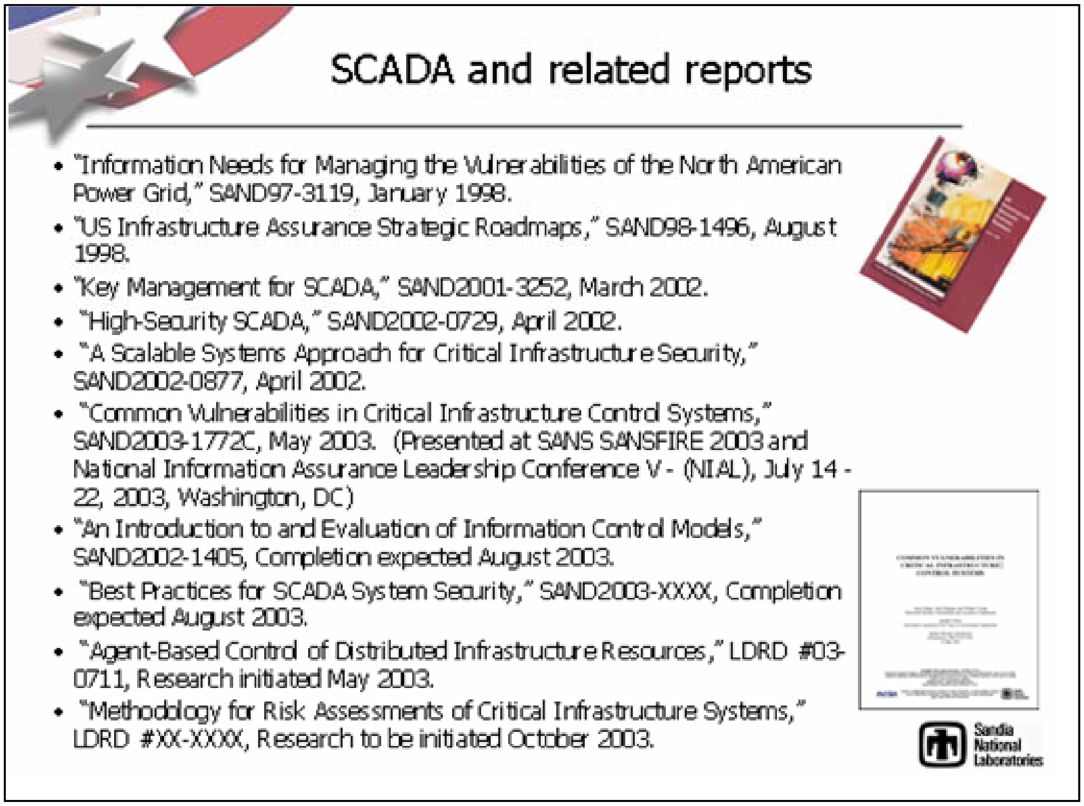
- A reconfigurable, portable SCADA system
- Comprised of five primary elements
- Using modern Digital Control System (or SCADA) components
- That has multiple uses
  - Security awareness demonstrations
  - Training tool
  - Red team attack development tool
  - SCADA protocol analysis tool
  - Security component evaluation tool

SSDS was developed under the IORTA program for its use and also use by both the Sandia SCADA and Distributed Energy programs

INFORMATION OPERATIONS RED TEAM & ASSESSMENTS
occulte oppugnare emendandi causa
IORTA
Sandia National Laboratories

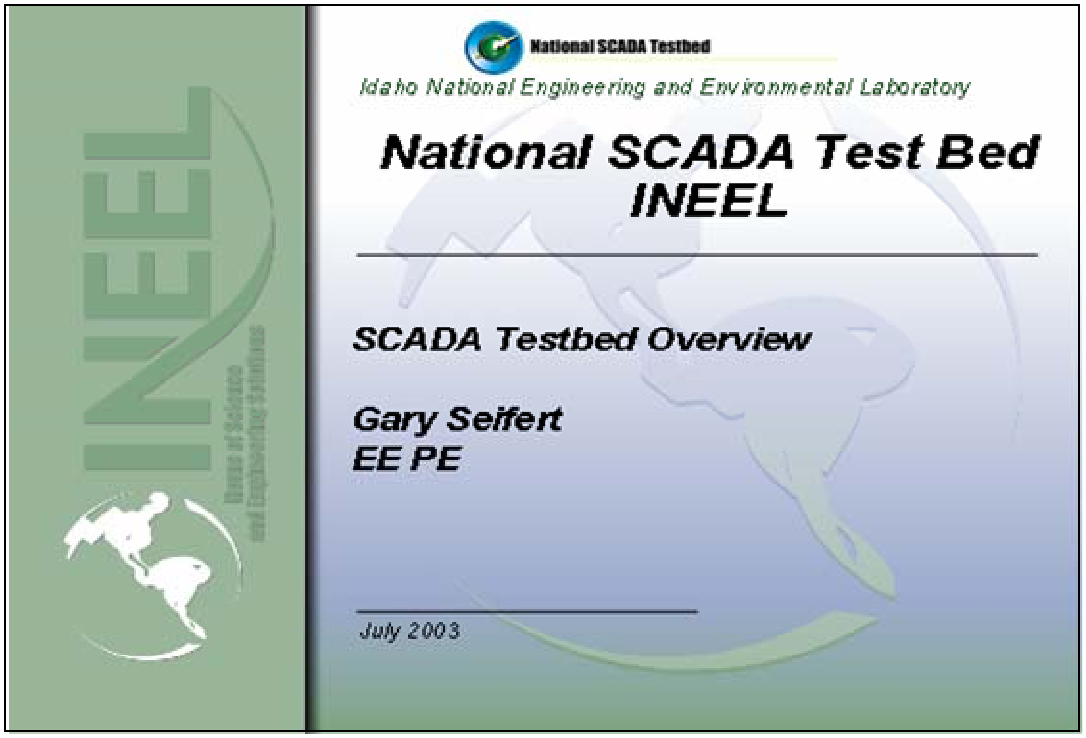


Projects and products



SCADA and related reports

- "Information Needs for Managing the Vulnerabilities of the North American Power Grid," SAND97-3119, January 1998.
- "US Infrastructure Assurance Strategic Roadmaps," SAND98-1496, August 1998.
- "Key Management for SCADA," SAND2001-3252, March 2002.
- "High-Security SCADA," SAND2002-0729, April 2002.
- "A Scalable Systems Approach for Critical Infrastructure Security," SAND2002-0877, April 2002.
- "Common Vulnerabilities in Critical Infrastructure Control Systems," SAND2003-1772C, May 2003. (Presented at SANS SANSFIRE 2003 and National Information Assurance Leadership Conference V - (NIAL), July 14 - 22, 2003, Washington, DC)
- "An Introduction to and Evaluation of Information Control Models," SAND2002-1405, Completion expected August 2003.
- "Best Practices for SCADA System Security," SAND2003-XXXX, Completion expected August 2003.
- "Agent-Based Control of Distributed Infrastructure Resources," LDRD #03-0711, Research initiated May 2003.
- "Methodology for Risk Assessments of Critical Infrastructure Systems," LDRD #XX-XXXX, Research to be initiated October 2003.


INEEL
House of Science and Engineering Solutions

National SCADA Testbed

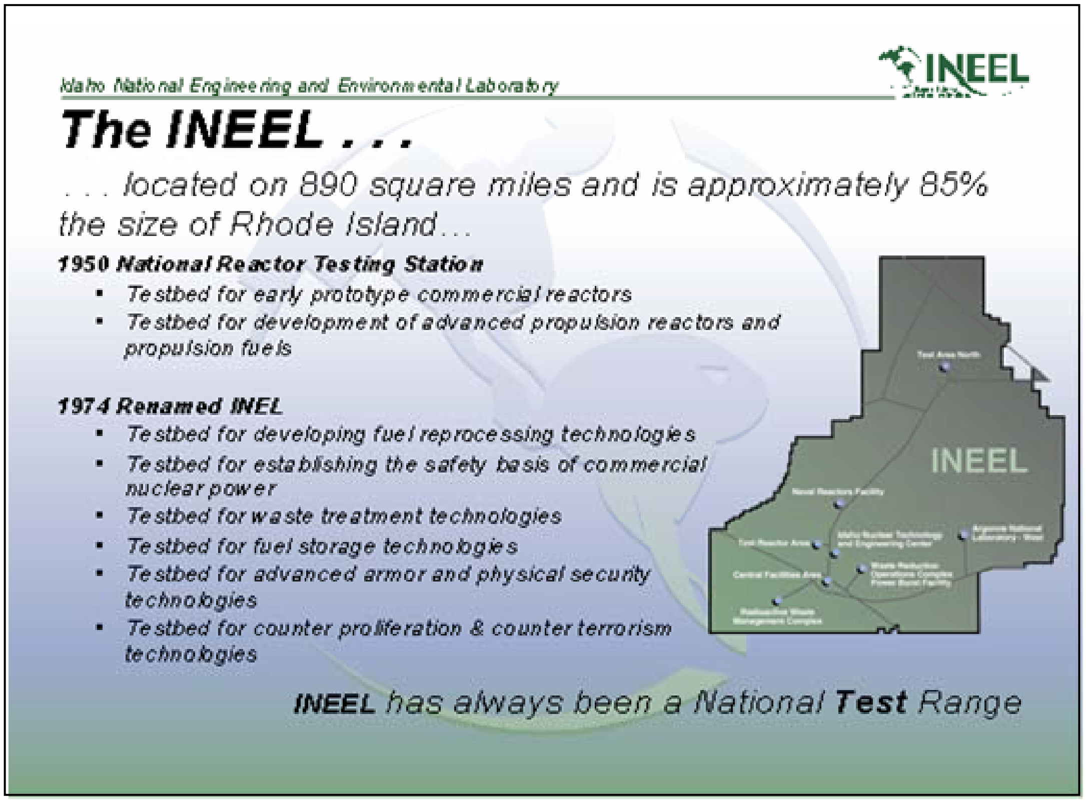
Idaho National Engineering and Environmental Laboratory

National SCADA Test Bed INEEL

SCADA Testbed Overview

Gary Seifert
EE PE

July 2003


INEEL
INEEL
Test Area North
Naval Reactors Facility
Idaho Nuclear Technology and Engineering Center
Argonne National Laboratory - West
Test Reactor Area
Central Facilities Area
Waste Reduction Operations Complex Power Burst Facility
Radioactive Waste Management Complex

Idaho National Engineering and Environmental Laboratory

The INEEL . . .

. . . located on 890 square miles and is approximately 85% the size of Rhode Island…

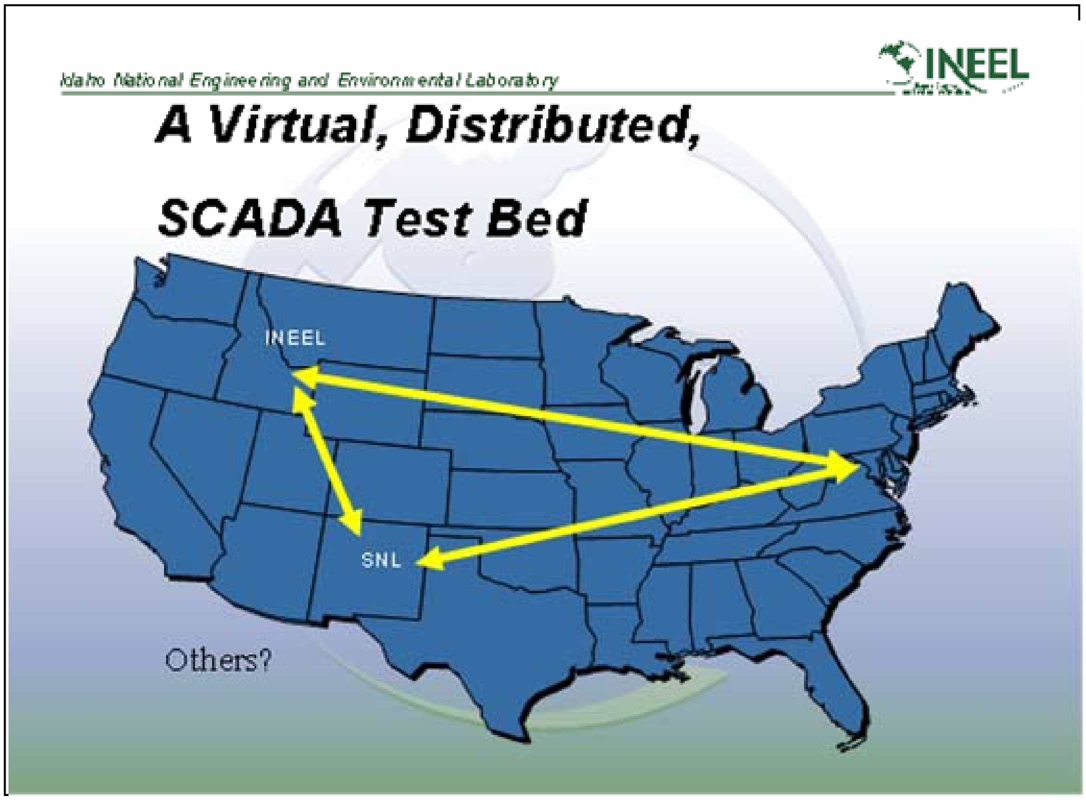
1950 National Reactor Testing Station

- Testbed for early prototype commercial reactors
- Testbed for development of advanced propulsion reactors and propulsion fuels

1974 Renamed INEL

- Testbed for developing fuel reprocessing technologies
- Testbed for establishing the safety basis of commercial nuclear power
- Testbed for waste treatment technologies
- Testbed for fuel storage technologies
- Testbed for advanced armor and physical security technologies
- Testbed for counter proliferation & counter terrorism technologies

INEEL has always been a National **Test** Range

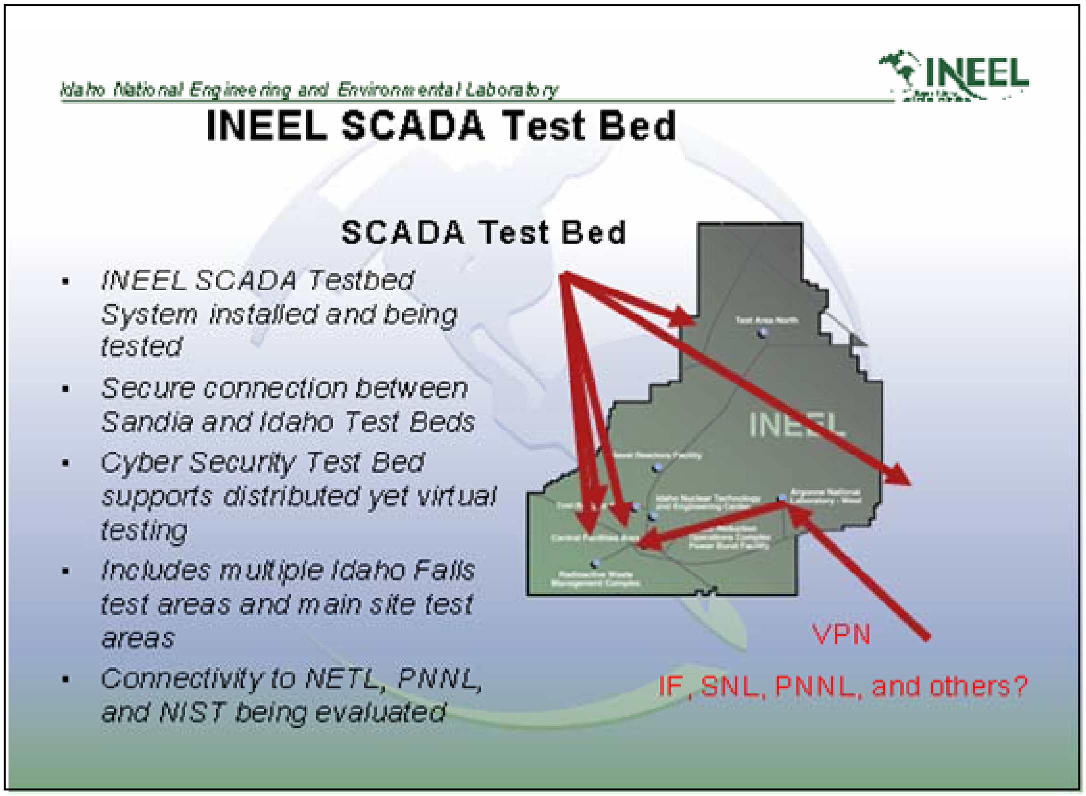


Idaho National Engineering and Environmental Laboratory

INEEL

A Virtual, Distributed, SCADA Test Bed

Others?



Idaho National Engineering and Environmental Laboratory

INEEL

INEEL SCADA Test Bed

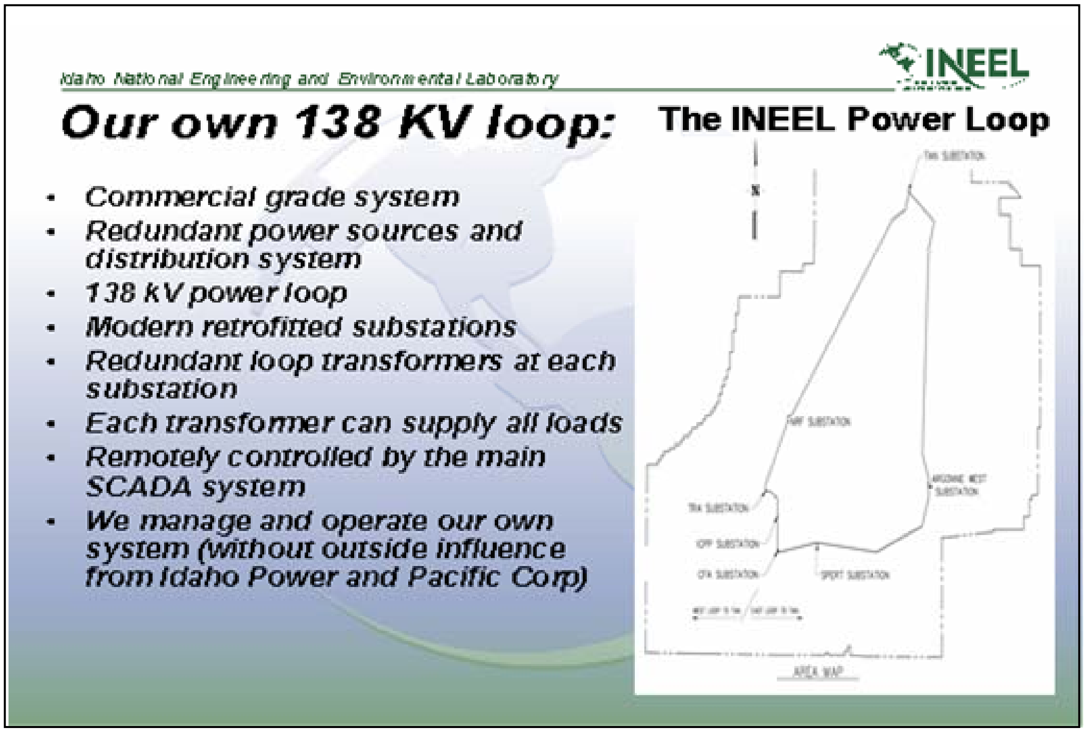
SCADA Test Bed

- INEEL SCADA Testbed System installed and being tested
- Secure connection between Sandia and Idaho Test Beds
- Cyber Security Test Bed supports distributed yet virtual testing
- Includes multiple Idaho Falls test areas and main site test areas
- Connectivity to NETL, PNNL, and NIST being evaluated

Test Area North
INEEL
Naval Reactors Facility
Idaho Nuclear Technology and Engineering Center
Argonne National Laboratory - West
Central Facilities Area
Operations Complex
Power Burst Facility
Radioactive Waste Management Complex

VPN

IF, SNL, PNNL, and others?

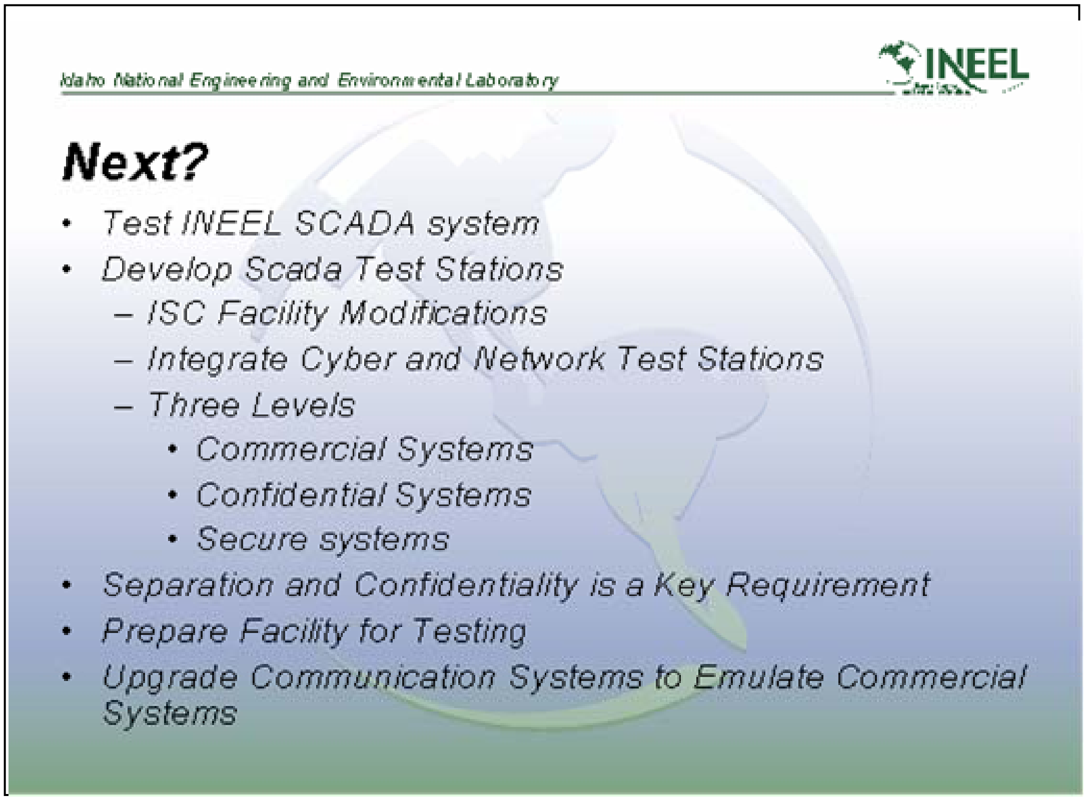


Our own 138 KV loop:

- Commercial grade system
- Redundant power sources and distribution system
- 138 kV power loop
- Modern retrofitted substations
- Redundant loop transformers at each substation
- Each transformer can supply all loads
- Remotely controlled by the main SCADA system
- We manage and operate our own system (without outside influence from Idaho Power and Pacific Corp)

The INEEL Power Loop

New Switchgear - Test Support

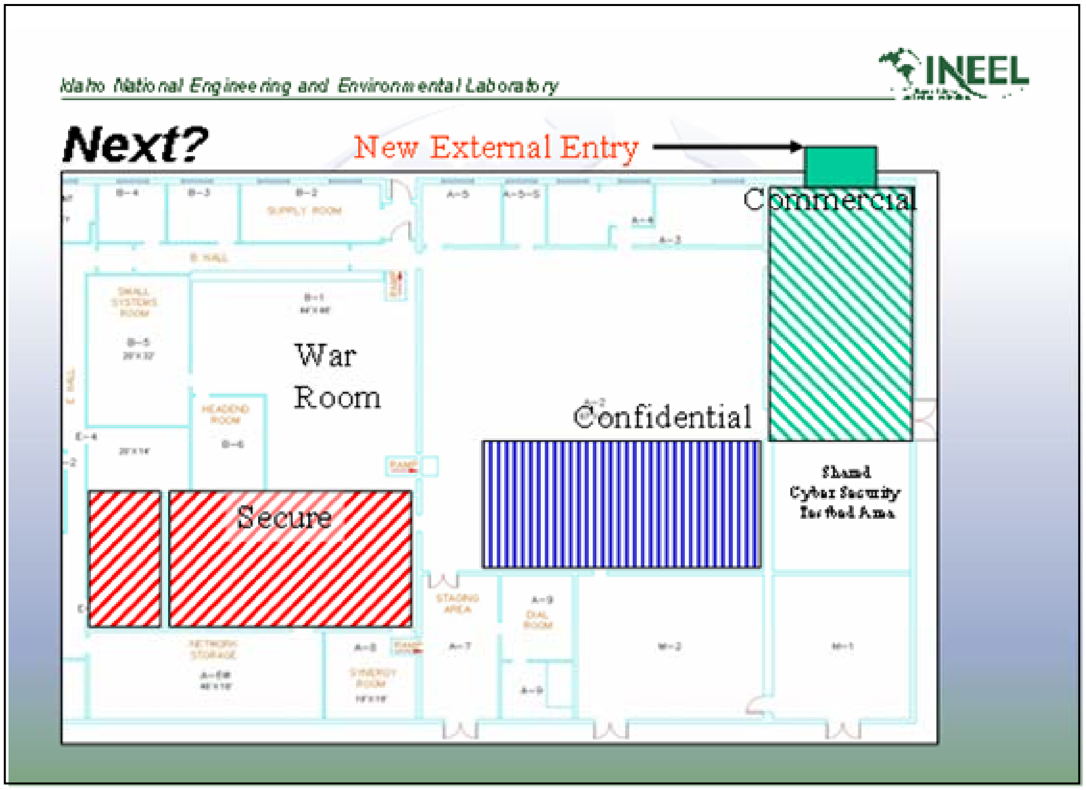


Idaho National Engineering and Environmental Laboratory

INEEL

Next?

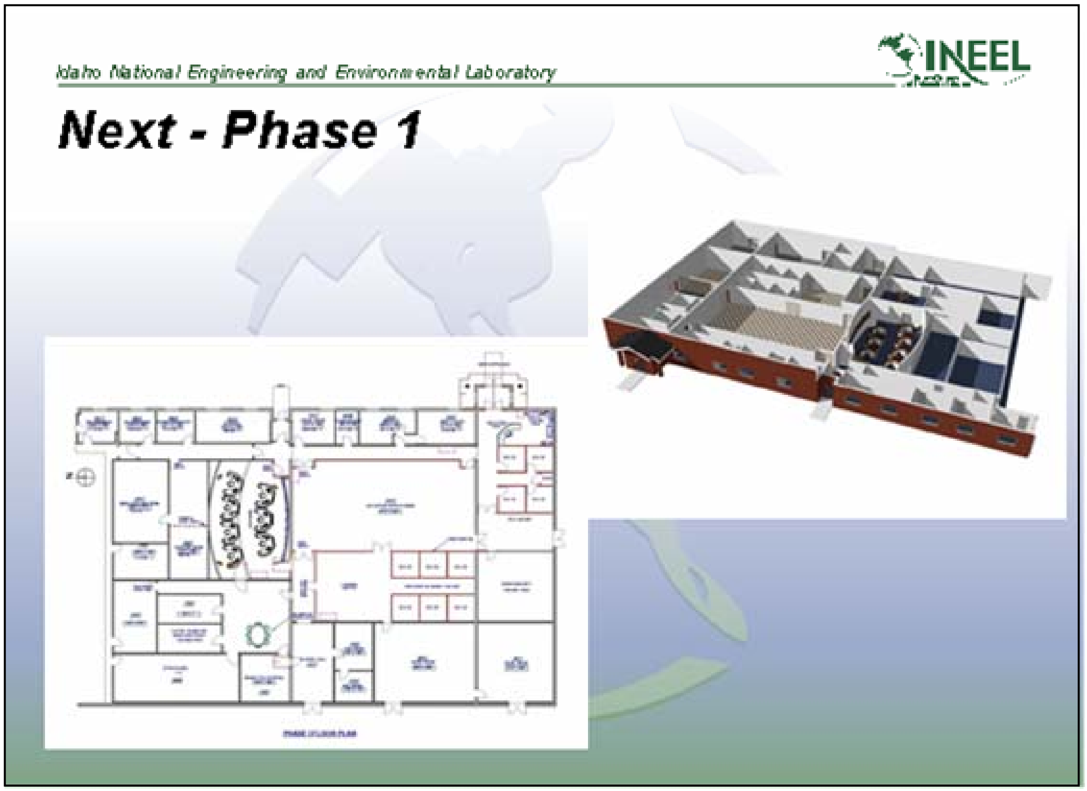
- Test INEEL SCADA system
- Develop Scada Test Stations
  - ISC Facility Modifications
  - Integrate Cyber and Network Test Stations
  - Three Levels
    - Commercial Systems
    - Confidential Systems
    - Secure systems
- Separation and Confidentiality is a Key Requirement
- Prepare Facility for Testing
- Upgrade Communication Systems to Emulate Commercial Systems



Idaho National Engineering and Environmental Laboratory

INEEL

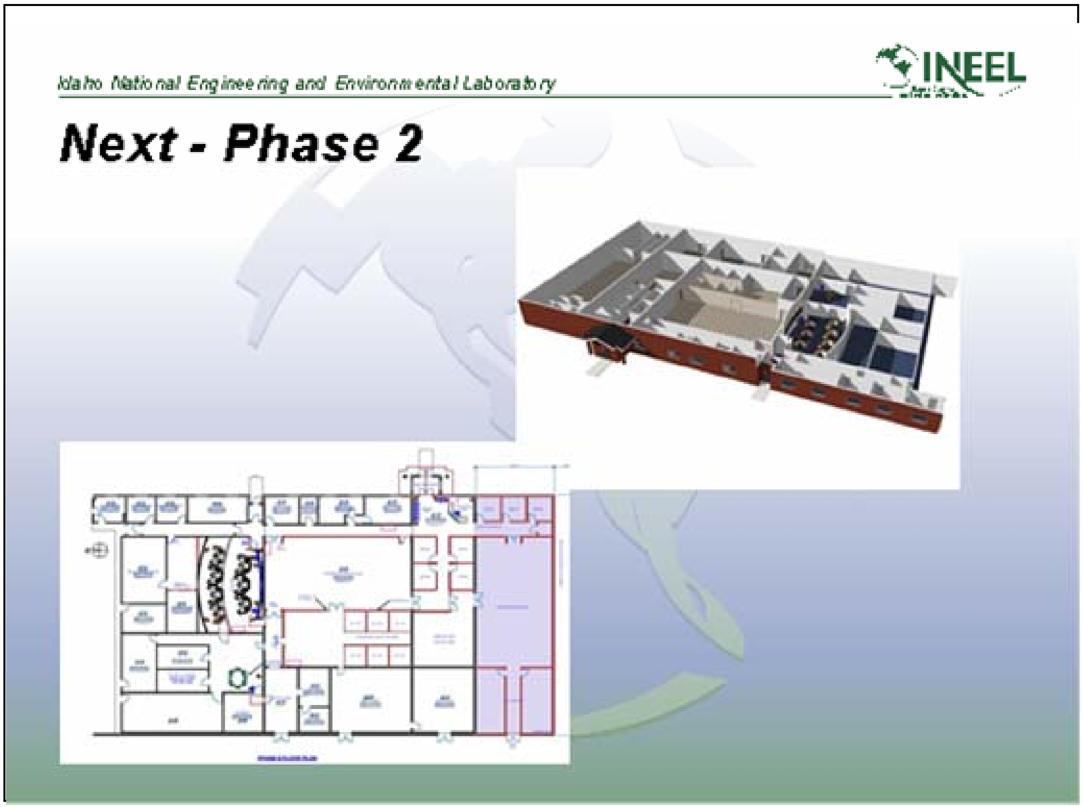
Next?



Idaho National Engineering and Environmental Laboratory

INEEL

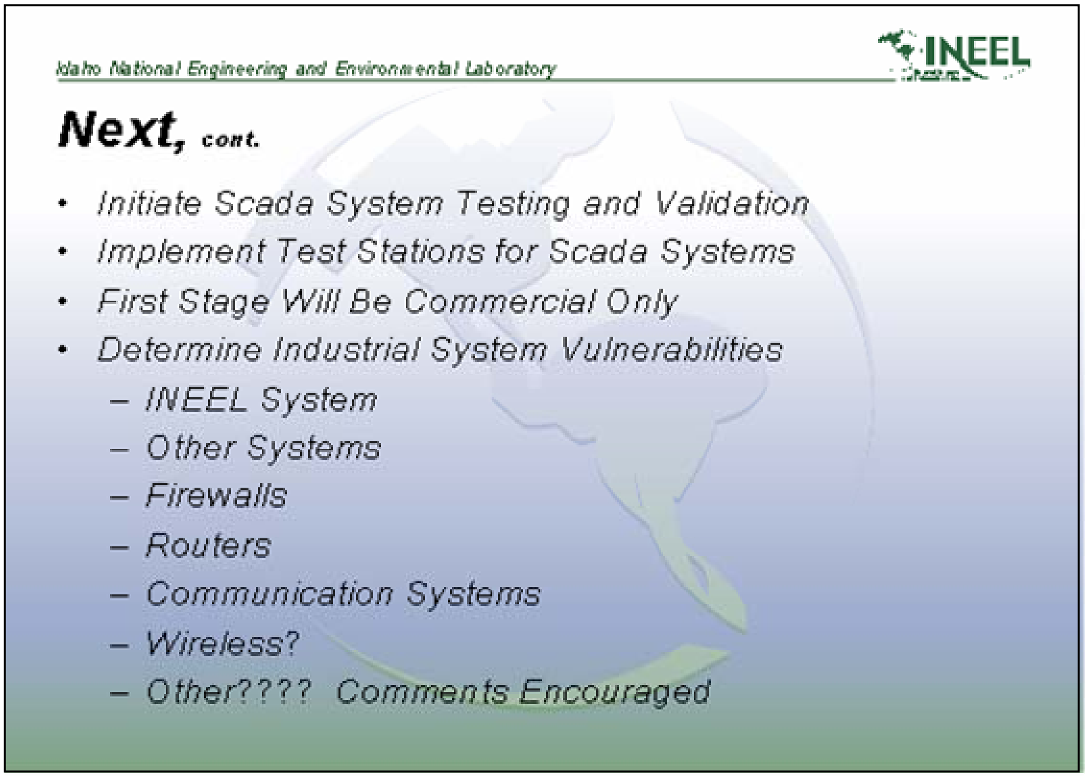
Next - Phase 1



Idaho National Engineering and Environmental Laboratory

INEEL

Next - Phase 2

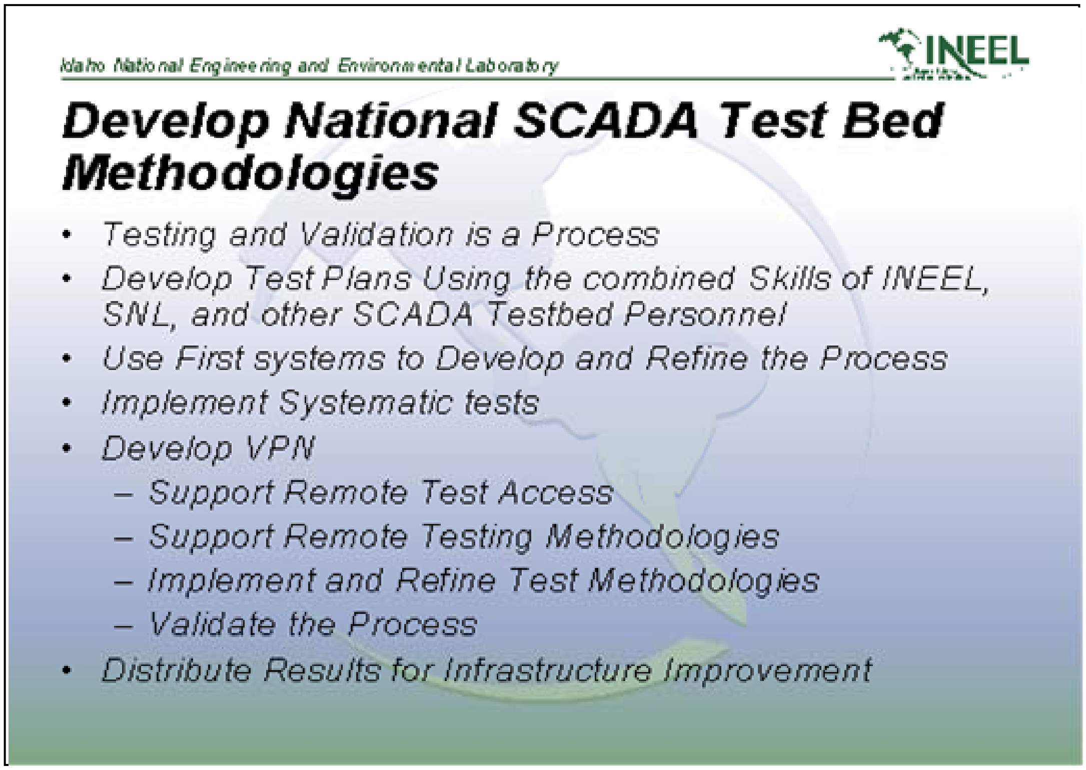


Idaho National Engineering and Environmental Laboratory

INEEL

Next, cont.

- Initiate Scada System Testing and Validation
- Implement Test Stations for Scada Systems
- First Stage Will Be Commercial Only
- Determine Industrial System Vulnerabilities
  - INEEL System
  - Other Systems
  - Firewalls
  - Routers
  - Communication Systems
  - Wireless?
  - Other???? Comments Encouraged

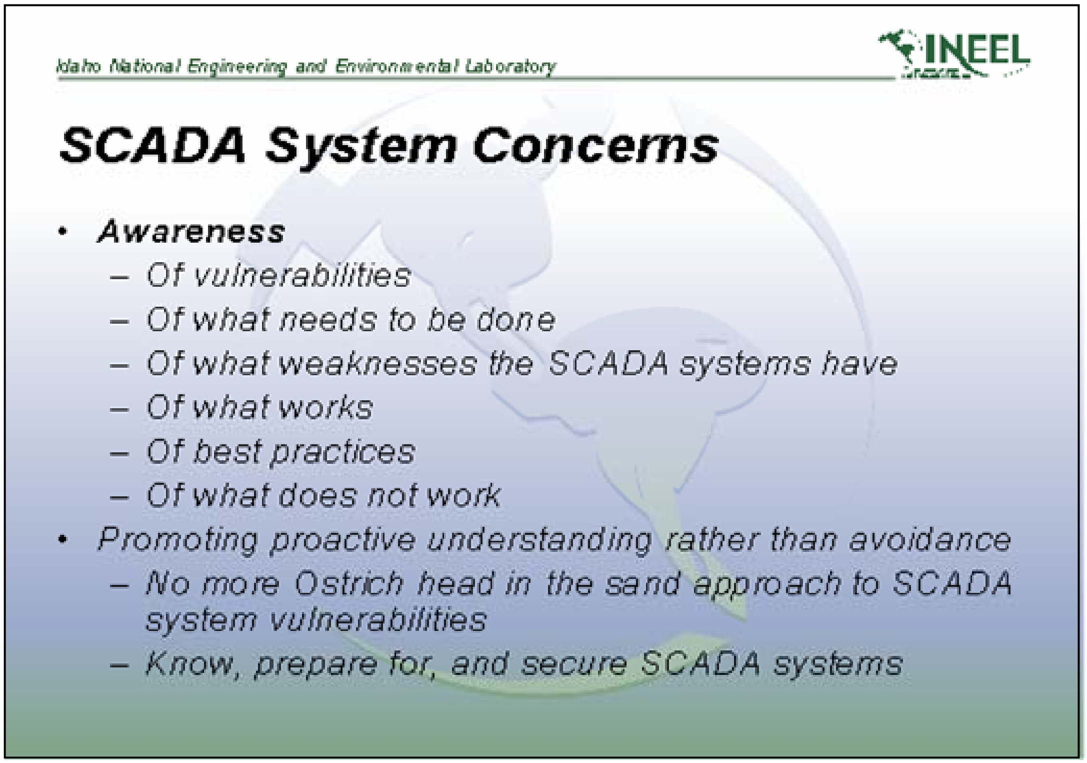


Idaho National Engineering and Environmental Laboratory

INEEL

Develop National SCADA Test Bed Methodologies

- Testing and Validation is a Process
- Develop Test Plans Using the combined Skills of INEEL, SNL, and other SCADA Testbed Personnel
- Use First systems to Develop and Refine the Process
- Implement Systematic tests
- Develop VPN
  - Support Remote Test Access
  - Support Remote Testing Methodologies
  - Implement and Refine Test Methodologies
  - Validate the Process
- Distribute Results for Infrastructure Improvement

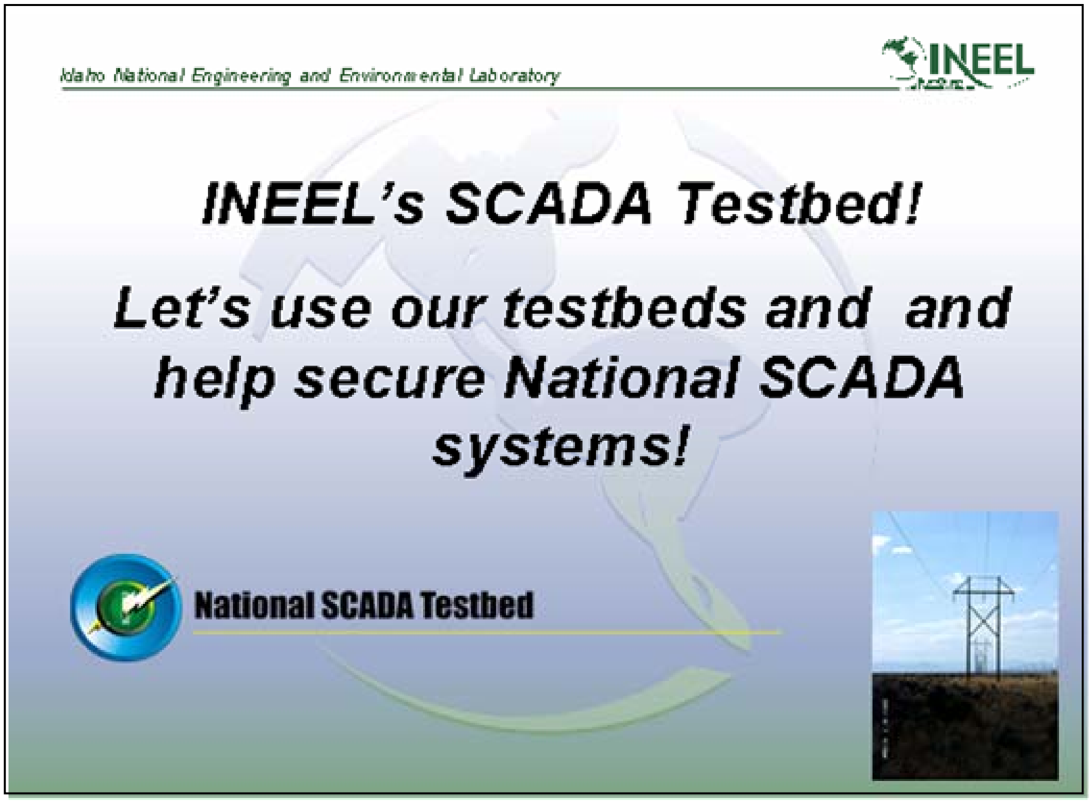


Idaho National Engineering and Environmental Laboratory

INEEL

SCADA System Concerns

- *Awareness*
  - *Of vulnerabilities*
  - *Of what needs to be done*
  - *Of what weaknesses the SCADA systems have*
  - *Of what works*
  - *Of best practices*
  - *Of what does not work*
- *Promoting proactive understanding rather than avoidance*
  - *No more Ostrich head in the sand approach to SCADA system vulnerabilities*
  - *Know, prepare for, and secure SCADA systems*



Idaho National Engineering and Environmental Laboratory

INEEL

INEEL's SCADA Testbed!

Let's use our testbeds and and help secure National SCADA systems!

National SCADA Testbed